Culture and Information Security

Outsourcing IT Services in China

Timo D. Glaser

Culture and Information Security

Outsourcing IT Services in China

February 3, 2009

Dedication

Deep cultural undercurrents structure life in subtle but highly consistent ways that are not consciously formulated. Like the invisible jet streams in the skies that determine the course of a storm, these hidden currents shape our lives; yet their influence is only beginning to be identified. Edward T. Hall, 1976

This thesis is dedicated to my parents for their endless support.

Berlin, February 2009   *Timo D. Glaser*

Acknowledgements

I would like to express my deep and sincere gratitude to my supervisor and personal mentor Prof. Bernd Lutterbeck. Bernd personifies interdisciplinary ideals and unconventional thinking in his research, teaching and personality. He inspired me to think beyond borders, to challenge assumptions, and enabled me to write a thesis that contributes to a new paradigm of security research. Moreover, Bernd gave me the opportunity to teach what I believe in, however crazy my ideas and concepts might have sounded. Through my teaching, he passed down part of his spirit not only to students in Germany but also in Accra, Ghana. Together, we planted a seed that will outlive all of us.

I am grateful to Prof. Hermann Krallmann for his clear assessment and guidance. He gave me the opportunity to broaden my knowledge in security research by conducting research at his chair. I had the privilege of working with outstanding security professionals at his information security management research group. Also at Prof. Krallmann's chair, I gained my first teaching experiences and could continuously challenge my ideas with researchers, practitioners and students.

I owe my most sincere gratitude to Frank Pallas, a colleague, sparring partner and friend. Like a surgeon, he identified deficiencies and provided suggestions that greatly improved my work. He is blessed with an incredibly analytical mind and his comments tremendously supported me in structuring my thesis. I could call him any time to talk about any problem and he always had a solution at hand. Most importantly, Frank boosted my motivation when I was down. Having him as a companion was invaluable to me.

During this work, I have also collaborated with many other colleagues for whom I have great regard. My sincere thanks are due to all colleagues at my chair, Computers & Society. Kei, Matthias, Kai, Karsten and many others formed a productive and inspiring working environment. Their constructive comments have been of great value.

This thesis would never have been possible without Prof. Günter Hommel and Prof. Sheng Huanye who started an exchange program between TU Berlin and Shanghai Jiao Tong University that offers an invaluable experience for German and Chinese students alike. It combines world-class teaching with a unique opportunity for personal growth. Especially the personal experience of living and studying in Shanghai formed me as an individual and is something that I will never forget. Even after I completed the program and started working on my PhD, Prof. Li Fang, Prof. Chen Kefei and especially Prof. Liu Shengli actively supported me. They gave me the chance to conduct research and teach in Shanghai. Shengli provided valuable guidance with her broad understanding of security issues and reflected insights into her own culture.

I would like to thank all my interviewees who generously offered their time and knowledge to support me throughout my work. I would like to give my special thanks to Jörg Heil (General Manager of hartung:consult Shanghai)

Abstract

With the rapid decline of communication costs, a decentralization of societies, businesses and information systems is taking place. Teleworking and outsourcing are two outcomes of this development. Due to this fundamental system transformation, traditional security concepts based on technical and organizational measures are not sufficient anymore. The human factor plays an increasingly important role. The influence of human behavior on information security needs to be properly addressed. Teleworking and outsourcing lead to growing information asymmetries between managers and their employees as well as companies and their outsourcing providers. This gap can be reduced by analyzing human behavior.

Recently, the integration of concepts from social sciences has started this thinking process. Economics and psychology are two research branches that are followed by security researchers. However, as a result of globalization, many corporations have become multicultural and outsourcing takes place on a global scale. Therefore, a profound understanding of cultural characteristics and the impact of culture on information security is crucial for bridging the information gap.

In the Chinese outsourcing market, this information gap is most evident. Managers are afraid of outsourcing their IT services within or even to China. They face the obstacle to judge the intention and quality of Chinese outsourcing providers. Furthermore, they are worried about the unstable environment and unknown cultural characteristics. By conducting research in the Chinese outsourcing and security industry, I have scrutinized whether this fear is justified. In this thesis, I thoroughly examine the Chinese outsourcing environment and analyze the impact of culture on information security. Therefore, I apply concepts from the discipline of cultural studies to security problems. I use Geert Hofstede's cultural dimensions to compare national cultures and to analyze their impact on information security. Moreover, I build on Edward T. Hall's work on intercultural communication to evaluate how cultural differences can endanger outsourcing deals. My observations of the Chinese environment are not limited to the outsourcing market. They include many insights that are relevant to anyone doing business in China. The findings on the impact of culture on information security are even more generic and independent of the country. They enhance our understanding of the human factor in information security. These observations reveal valuable insights that are necessary for managing security risks.

Analyzing human behavior in order to manage security risks is an approach that can directly be applied and will be followed in the next one or two decades. In the long run, information security needs a fundamental change. As societies, businesses and information systems have transformed from isolated entities to hierarchical structures to decentralized systems, information security strategies eventually need to make this last step as well. Gathering more and more information will help decision makers to obtain a clearer pic-

ture. With more knowledge, they become able to better regulate the system. However, as with political and economic systems, security managers cannot gather an infinite amount of information which would be necessary to regulate highly decentralized systems. Eventually, we need a market mechanism in information security that regulates in form of Adam Smith's invisible hand. Until then, my thesis adds an important jigsaw piece to the analytical toolbox of security and risk managers.

Zusammenfassung

Sinkende Kommunikationskosten ermöglichen die Dezentralisierung von Gesellschaftsstrukturen, Unternehmen und Informations- und Kommunikationssystemen. Zwei Folgen dieser Entwicklung sind mobile Mitarbeiter und die Auslagerung von Geschäftsprozessen. Aufgrund dieser fundamentalen Veränderungen in der Arbeitswelt sind klassische Sicherheitskonzepte nicht mehr ausreichend. Der Einfluss des Verhaltens der Mitarbeiter auf die Informationssicherheit in Unternehmen muss ausreichend verstanden und adressiert werden. Telearbeit und Outsourcing führen zu wachsenden Informationsasymmetrien zwischen Managern und ihren Mitarbeitern sowie Firmen und ihren Dienstleistern. Diese Asymmetrien können durch die Analyse des menschlichen Verhaltens verringert werden.

In den letzten Jahren hat die Integration von geisteswissenschaftlichen Konzepten in die Sicherheitsforschung diesen Denkprozess angestoßen. Ökonomie und Psychologie sind zwei Pfade, welche Wissenschaftler in diesem Zusammenhang eingeschlagen haben. Im Rahmen der Globalisierung haben sich viele Unternehmen jedoch zu multinationalen Konzernen entwickelt, Outsourcing von Produktion und Dienstleistungen findet längst auf internationaler Ebene statt. Aus diesen Gründen wird ein tiefgreifendes Verständnis unterschiedlicher kultureller Charakteristika immer bedeutender. Nur mit diesem Hintergrundwissen kann der Einfluss von Kultur auf Informationssicherheit analysiert und somit die Informationsasymmetrie reduziert werden.

Am deutlichsten werden die Probleme der Informationsasymmetrie, wenn man den chinesischen Outsourcingmarkt betrachtet. Manager haben Angst ihre IT-Services innerhalb bzw. nach China auszulagern. Sie stehen vor dem Problem die Intention und Qualität chinesischer Outsourcingdienstleister bewerten zu müssen. Darüber hinaus fürchten sie instabile Rahmenbedingungen und die unbekannte Kultur. Durch empirische Forschung in der chinesischen Outsourcing- und Sicherheitsindustrie habe ich analysiert, ob diese Befürchtungen gerechtfertigt sind. Ich betrachte die Rahmenfaktoren für Outsourcing in China und untersuche darüber hinaus den Einfluss nationaler Kulturen auf Informationssicherheit. Hierfür adaptiere ich kulturwissenschaftliche Methoden und Konzepte und wende sie auf Probleme der Informationssicherheit an. Ich nutze Geert Hofstedes Kulturdimensionen, um nationale Kulturen zu vergleichen und ihren Einfluss auf die Informationssicherheit zu bewerten. Darüber hinaus evaluiere ich auf Basis von Edward T. Halls Arbeit über interkulturelle Kommunikation inwiefern kulturelle Unterschiede Outsourcingvorhaben gefährden. Meine Betrachtung der chinesischen Rahmenbedingungen ist nicht auf den Outsourcingmarkt beschränkt, sondern umfasst viele Aspekte die für jeden Geschäftstreibenden in China von Bedeutung sind. Die Erkenntnisse bezüglich der Zusammenhänge zwischen nationalen Kulturen und Sicherheitsrisiken gehen nicht nur über das Thema Outsourcing hinaus, sondern lassen sich auch auf andere Nationen und Kulturkreise übertragen. Die Analyse dieser Zusammenhänge dient der Verbesserung des Verständnisses

des Faktors Mensch in der Informationssicherheit. Die Betrachtungen offenbaren wertvolle Erkenntnisse, die notwendig sind, um sich umfassender gegen Sicherheitsrisiken zu schützen.

Die Analyse des menschlichen Verhaltens zur Verbesserung der Informationssicherheit ist ein Ansatz, der unmittelbar angewendet werden kann. Er wird meines Erachtens in den nächsten ein bis zwei Jahrzehnten verfolgt werden. Langfristig muss jedoch ein fundamentales Umdenken in der Sicherheitsforschung und -praxis stattfinden. Mit der Transformation von Gesellschaftsstrukturen, Unternehmen und Informations- und Kommunikationssystemen von isolierten Einheiten über hierarchische Strukturen bis hin zu dezentralisierten Systemen müssen auch Sicherheitsstrategien dieser Entwicklung angepasst werden. Die verstärkte Aggregation von Informationen wird Entscheidern in den nächsten Jahren helfen ein klareres Bild der Zusammenhänge zu erlangen. Ein umfänglicheres Wissen wird sie in die Lage versetzen die Systeme besser zu regulieren. Genau wie bei politischen und ökonomischen Systemen ist es jedoch auch Sicherheitsmanagern nicht möglich eine unbegrenzte Menge an Informationen aufzunehmen und zu verarbeiten. Dies wäre für die Regulation hochgradig dezentralisierter Systeme notwendig. Auf lange Sicht sollten wir einen Marktmechanismus in der Informationssicherheit etablieren, welcher eine Regulation in Form von Adam Smiths unsichtbarer Hand ermöglicht. Bis dieser Mechanismus gefunden und etabliert ist, wird die vorliegende Arbeit ein wichtiges zusätzliches Element für die Arbeit von Sicherheits- und Risikomanagern darstellen.

Contents

Part II The Chinese Outsourcing Environment

Part III Cultural Security Issues in China

Part IV Conclusion

Appendix

1

Introduction

In recent years, China's visibility as an outsourcing destination has increased rapidly. However, many foreign managers are afraid of outsourcing IT services within or even to China. They worry about the unknown business environment and cultural differences. The behavior of Chinese employees is hard to understand or even to predict. Since the human factor is gaining importance in information security, assessing the quality of Chinese outsourcing providers is becoming more difficult. This thesis shines light on two major issues. First, it scrutinizes the Chinese outsourcing environment and thereby illuminates whether the managers' fear is justified. Second, it applies concepts from social sciences, especially from cultural studies, to information security problems. As a result, insights on the impact of human behavior on information security are gained. Culture does play a major role in information security and this role is deciphered in the course of this thesis. With this thesis, I hope to find the proper balance between practice and research. I strive to provide valuable information to professionals doing business in China and researchers trying to understand the impact of culture on information security.

1.1 Outsourcing IT Services – A Market for Lemons?

The Chinese outsourcing market feels like a *market for lemons*.[1] Outsourcing providers deliver low quality services. Managers are afraid of outsourcing IT services in and to China. The entire market seems immature. If we look at other countries and their outsourcing markets, similar problems exist as well. Only very few providers offer, what we might call, secure services. Distrust is a general problem of the outsourcing market. However, this problem is worse in China.

Looking into the field of economics, we find an explanation for the lack of high quality outsourcing providers. This explanation also helps us to un-

---

[1] See Akerlof (1970)

derstand why the problems in China are worse than in many other countries. There is one major reason for the lack of secure providers – the information asymmetry of outsourcing services. Outsourcing clients face the *principal-agent problem*. Providing secure services is costly for the outsourcing provider and it is difficult for the client to assess the provider's quality level. Information asymmetries and the principal-agent problem are not limited to the outsourcing industry. In fact, they can be conceived best by looking at other fields. Anderson and Moore describe the same problem for the software market as follows:[2]

> Vendors may make claims about the security of their products, but buyers have no reason to trust them. In many cases, even the vendor does not know how secure its software is. So buyers have no reason to pay more for protection, and vendors are disinclined to invest in it.

The outsourcing market faces exactly the same problem. Since clients can hardly judge the level of security an outsourcing provider offers, they are not willing to pay for it. So why should providers bother reaching a high level of security? *"Fail to solve [this] economic problem, and vendors will not bother implementing [...] any security technologies, regardless of how effective they are."*[3] If we cannot judge the quality of a product or service, bad services will drive out the good.[4] This rises the question of how this effect is usually being counteracted – how the market is stabilized.

Michael Spence and Joseph Stiglitz, who received the 2001 Nobel Prize in Economics together with George Akerlof, propose two solutions – *Signaling* and *Screening*.[5] Signaling means that one party provides some kind of proof of its quality. In the job market, this can be a degree from a prestigious university. A certification fulfills the same purpose in the outsourcing industry.[6] Screening means that the outsourcing client collects information about potential providers and thereby reduces the information asymmetry. I will come back to these two methods later on. Akerlof further suggests two institutions that can solve the principal-agent problem.[7] The institutions he refers to are *guarantees* and *brand names*. Service Level Agreements, a very common component of outsourcing deals, can be seen as guarantees in the outsourcing world. With a Service Level Agreement in place, both parties agree on a certain level of service quality. If that quality level is not maintained, the provider has to pay financial penalties to its client. The second institution, brands, rests upon the trust in the quality of a service provider based on its reputation. Companies that can afford paying a premium price often choose

---

[2] See Anderson and Moore (2006, p. 612)

[3] See Schneier (2007, p. 4)

[4] This is an adaption of Gresham's law. See Akerlof (1970, p. 490)

[5] See, for example, Spence (1973, 1974) and Stiglitz (1973)

[6] ISO/IEC 27001, for example, is meant to attest the security level of an organization. ISO 9001 has the same role in the field of quality management.

[7] See Akerlof (1970, p. 499)

international providers because of their reputation.[8] These providers have an economic incentive to provide high quality services. If they would not provide the service quality that their clients expect, their brand would suffer. A loss of image might not only effect their operations in the Chinese market but also their success in other countries.

Let me summarize these insights and explain why the situation is worse in China than in other countries. Information asymmetries, and the resulting uncertainty, lead to a market of low quality service providers. The IT outsourcing market is such a market for lemons. There is an information asymmetry between providers and their potential clients that is hard to resolve. Companies cannot accurately assess the quality of service providers even though these providers can assess their own quality fairly well. If outsourcing clients realize that providers pretend to offer higher quality services than they actually do, they are not willing to pay the same price anymore. Even if they change providers, they might lower the price they are willing to pay because they expect similar problems and still cannot properly assess the quality of the new provider. Because the information asymmetry is linked to the services offered, this is a general problem in the entire outsourcing industry. However, the situation is worse in China. There are various reasons that explain this assessment. Akerlof claimed in 1970 that *"dishonesty in business is a serious problem in underdeveloped countries"* and that *"quality variation is a greater problem in the East than in the West"*.[9] This judgement has not changed much in the past forty years. Furthermore, there are a couple of practical problems that impair the uncertainty that clients face and therefore worsen the situation in China. In order to analyze these, I would like to go through the four ways of solving the principal-agent problem once again – *brands*, *signaling*, *guarantees* and *screening*. The brand is the only method that functions in China almost in the same way as in other countries. However, many Chinese brands are not known by foreign companies. Furthermore, an American brand can be diluted if key account managers, or even the managing director of the Chinese subsidiary, are not foreigners but Chinese. While employing locals makes sense from an business point of view (lower salaries, better communication with employees, extensive market knowledge, etc.), it can undermine the American image of the company if it is represented by a Chinese, regardless of how qualified he or she might be. Despite these problems, brands are still a very common criteria that is used for provider selection. A signal is comparable to a brand but more tangible. Signaling normally refers to certificates, provided by a neutral third party that attest a certain level of quality. In China, certifications are still pretty rare. Very few companies obtain certificates and potential customers worry about their validity. They are afraid that providers received

---

[8] Even though the service quality of international providers seems to be slightly higher than for their domestic Chinese counterparts, the quality they provide in China is still rather low.

[9] See Akerlof (1970, p. 495 f.)

those certificates due to good relations rather than based on serious audits. Certificates are often compared to degrees and job references. In China, a large number of people apply for jobs with faked credentials. This also dilutes the trust in information security and quality management certificates. The objections to guarantees are similar. Service Level Agreements are meant to reassure clients because they can penalize their outsourcing providers if those do not comply with the service level that both parties agreed on. In reality, however, many providers do not stick to their Service Level Agreements. This is partly due to cultural differences and a different understanding of the intent of a contract. In Chinese culture, contracts are seen as a description of the status quo rather than a legally binding document. If the situation changes, the contract is not valid anymore in its former specifics. Problems with Service Level Agreements also arise as a result of deficiencies in the Chinese legal system. As a foreign company it is extremely hard to sue Chinese providers (especially if they are state-owned) and to enforce Service Level Agreements. In the end, it might not matter that it was formally signed by both parties and that the provider violated it.[10] Screening is the last option that companies can pursue to overcome the principal-agent problem. Providers can be evaluated (screened) based on various characteristics. However, also this *due diligence* process is more difficult to conduct in China than in many other countries. Language barriers, lack of standardized processes and certifications as well the difficulty of background screens make due diligence extremely hard. Evaluating an outsourcing provider's staff is almost impossible. The human factor, which plays an increasingly important role in information security, is hard to assess. This raises the uncertainty that companies face. The information asymmetry between them and potential outsourcing providers is difficult to reduce, especially in China.

Managers do not trust the rules of the Chinese market because it seems very foreign to them. They do not trust the fruits that are sold on this market because they cannot distinguish between different kinds. Because they do not know if they buy a lemon or a cherry, they are afraid of paying a price that the market needs to function. Because of their unwillingness to trust the market and to trust individual providers, mostly sour providers survive. With the human factor gaining importance, the level of information security becomes harder to assess. All this turns the outsourcing market into a market for lemons. In China, but to a lower extent all over the world, outsourcing services are sold mostly based on trust. Without more insights into the Chinese outsourcing market and without a way to analyze the impact of human behavior on information security, the outsourcing market in China will stay a market for lemons.

---

[10] For an in-depth description of the Chinese legal system and resulting problems, see section 4.3

1.2 From a Specific Problem to My Research Question (and Beyond)

Motivated by the business needs of companies that consider outsourcing their IT services in or to the People's Republic of China, I began my research quest. These companies are looking for a way to analyze and manage security risks threatening outsourcing projects in China. The following fundamental questions started my research:

> Why are managers so scared of outsourcing IT services within and to China? How can companies analyze and manage security risks posed on outsourcing projects in China?

A framework for structuring and analyzing potential security threats of outsourcing deals in China would be a first step to help managers in their decision making process. However, such a framework would only scratch the surface of the real problem.[11] I realized that many issues, like the information asymmetry, can hardly be addressed by a decision making framework. By looking at existing frameworks, I realized that they were too generic. They were a good starting point but could not provide valuable information on outsourcing in China in particular. In order to find out which aspects play an important role in making managers believe that outsourcing in China is dangerous, one needs to answer the fundamental question of what kinds of risks exist while outsourcing in or to China. I realized that I had to get on the ground in China and collect data to understand the real problems companies face.

By conducting semi-structured interviews in China,[12] I derived a long list of outsourcing risks. This list exposed two interesting aspects. First, it strengthened my belief that the initial questions were too broad because security risks related to outsourcing activities in China are manifold. There are many reasons why managers are afraid of outsourcing in China. Security risks are one important aspect. But even security risks are still a very broad field that needs to be dissected. Second, the research results show (or rather verify) that culture-related security risks play an important role in the fear of professionals who consider outsourcing in China. While talking to many foreign and local managers at outsourcing providers and companies that would like to outsource their IT services, I noticed that the topic of culture always came up as a major problem. The impact of culture is hardly understood up to now. By narrowing down my initial research question to the aspect of culture, I derived a specific and highly important research task. Answering the question of how to manage culture-related security risks while outsourcing in China

---

[11] There are already a couple of frameworks that help managing the outsourcing process. Their focus lies on due diligence, the analysis of potential outsourcing providers before selecting one or a few of them.

[12] See appendix A

helps companies in their outsourcing efforts and generates knowledge about human behavior and its impact on information security. The specific and final research question that the rest of this research is based on can be phrased as follows:

> How can companies predict, evaluate and manage security risks that occur due to cultural characteristics while outsourcing in China?

In order to answer this question, I needed a framework. I needed an approach that helped to structure my thoughts but also to generate ideas about how to solve this problem. Directly looking for solutions that can solve the problem would be like looking for a needle in a haystack. All one could do would be to observe other companies with similar problems and select a solution, a best practice, that fits one's specific needs. However, I wanted to answer the question on a more generic level, not only for a single company. I needed to find a specific solution to a specific question but not a specific solution to the problems of a single company. I was looking for a generic approach. Therefore, I decided to follow the generic problem solving model which is shown in figure 1.1. The first step of this model, after being confronted with a real world problem, is to raise it to a more generic level. After this intermediary step, one can find a generic solution to the generic problem. By adapting this generic solution to the specific problem one can derive a specific solution that answers the question not only for a single company but on a more generic level.

Fig. 1.1. Generic Problem Solving Model – Scientific Circle

In the following, I describe how I followed this model. My process is visualized in figure 1.2. I will refer to the *Generic Problem Solving Model* as *Scientific Circle* from now on.

My first step was to follow the scientific circle upwards, looking for the generic problem overarching my specific one. Thereby, I could later find a

Fig. 1.2. Scientific Circle as followed by this Thesis

generic solution. This generic solution led to a specific solution which solved my specific problem. The generic problem that I identified was that the impact of culture on information security has not properly been examined up to now. By following the scientific circle, I needed to find an generic solution that solved this generic problem. I had to find a structured way to analyze and predict culture-based security threats. Therefore, I conducted a broad literature review in the field of cultural studies. Since I was addressing cultural issues, and the field of information security did not offer any explanations, this was the most appropriate starting point. I soon found an interesting field that offered a promising framework. I found that one possible solution to my generic problem is to use dimensional cultural models.[13] These models explain cultural characteristics by clustering their underlying principles into a few dimensions. These dimensions can be used for analyzing and comparing cultures. Some researchers have even derived scores for each dimension in various different countries and thereby offer a quantitative model for comparing national cultures. Those dimensional cultural models can also be used to analyze security risks related to cultural characteristics. Looking at cultural characteristics of own employees and the employees of potential outsourcing providers, companies which would like to outsource some of their services can

---

[13] See chapter 5

anticipate potential culture clashes and manage culture-related security risks – thereby solving the specific problem. This is exactly what I did during the last few years and what I will present in the course of this thesis.

1.3 Scientific Approach

After having provided a broad – rather anecdotal – overview of my research process, I would like to substantiate it now scientifically by briefly describing my research methodology.

The research I conducted can be called *qualitative exploratory research*. It is inherently interdisciplinary. I use qualitative methods from social sciences in order to gain insights into outsourcing partnerships and related information security issues. Initiated by a feeling and anecdotal evidence that there is a relation between culture and information security, at least in China, I started exploring this field. I started my research process without a pre-defined research hypothesis. Following a hermeneutic research philosophy, I believe that one can never fully understand a research problem. One can only enhance one's understanding of the problem and the entire context surrounding it. Since the intersection of culture and information security is an entirely new research field, research hypotheses and findings can only be based on empirical data. I collected this data by conducting *problem-centered interviews*. From August to December 2006, I interviewed 38 professionals with a background in information security and outsourcing (outsourcing clients and outsourcing providers), as well as people with related professions like external auditors and lawyers. All these interviews were conducted in China. For collecting and analyzing the data, I followed a research strategy that is best described as *grounded theory*. In order to increase the trustworthiness of my findings, I triangulated (or rather crystallized) my results with studies from other fields and cross-checked qualitative data with quantitative surveys. Most helpful were studies from the field of air traffic safety.

However objective I tried to approach my research problem, it will always inherit my own personal bias. This bias is present in my research methodology and also in my research findings. This is no flaw of my research but rather a limitation that is always part of every kind of research. Unfortunately, researchers often forget or conceal their personal bias so that readers forget about it. The bias is unproblematic as long as the reader is aware of it and keeps in mind that the author's culture and personality are inherited in his or her research.

Readers interested in more details on my research methodology can refer to appendix A. It contains an entire chapter on my methodology and the reasons for my selection of particular scientific methods.

1.4 Scope and Structure of the Thesis

As mentioned earlier, this thesis covers aspects of three main topics: *Information Security*, *Outsourcing*, and *Culture*.[14] It is about security issues that come up while outsourcing in China. While conducing interviews and analyzing outsourcing risks that companies face in outsourcing deals, it became obvious that culture plays a central role. This thesis starts with an introduction to information security and outsourcing (1).[15] Afterwards, I provide information on the Chinese outsourcing environment and analyze the intersection between culture and information security (2). I build a model for analyzing and predicting security threats based on cultural characteristics. Those results are derived from insights I gained in the outsourcing industry. They can be used by researchers and practitioners in the fields of outsourcing and information security to understand the influence of culture (3). Outsourcing is the scope I chose for analyzing the impact of culture on information security. China is the country I mainly focused on for understanding those cultural issues. China can therefore be seen as the glasses, the perspective, through which we look at all three research fields and their intersections.

Fig. 1.3. Intersection of my Topics

---

[14] See figure 1.3
[15] See figure 1.3

The structure that I follow is based on these considerations. In the following, I would like to explain this structure in a little more detail.[16] The thesis is divided into three main parts. To round up these three parts, I added an introduction and a conclusion. In the introduction, I present my motivation for starting this journey. It reveals my urge to understand why China's outsourcing market is a market for lemons. It also shows the goals, the research approach and the structure of this thesis. Afterwards, in part one, I introduce basic definitions and developments in the fields of information security and outsourcing. I not only describe general developments in these field but also give first insights into outsourcing in China in particular. I describe China's preconditions for outsourcing and sketch out current and future developments in its outsourcing market. Part one builds the foundation for all later chapters. The rest of the thesis is about the empirical research I conducted and my research findings.

Looking at outsourcing risks in more detail, they can be divided into three levels. Risks can exist on an environmental level, an organizational level and an individual/group level.[17]

Fig. 1.4. Levels of Security Research

I focus on the environmental level and a part of the individual/group level. The organizational level is specific to particular outsourcing providers and therefore not generic enough. I therefore excluded this level from this thesis.[18] The environmental level is broader than the organizational level. It is only specific to the country. It is described in part two of this thesis. Part two focuses on security risks (on an environmental level) that companies face while outsourcing within and to China. Examples are stability issues, the legal conditions in China, its infrastructure, etc.

The third part of this thesis is about the intersection of information security and culture. It analyzes security issues on the individual/group level

---

[16] See figure 1.5 for a detailed visualization of the structure of this thesis, including its parts and chapters.

[17] See figures 1.4, 1.5 and 4.1

[18] For more information, see also section 4.1

with a strong focus on culture. Please note that culture is only one part of the individual/group level. However, during my interviews, it crystallized as the most crucial aspect. It is the factor that my interviewees were most worried about. Another reason for focusing on culture is the consideration that human nature is identical for every individual. Understanding human nature is important for understanding security issues but since it does not vary from country to country, it does not provide insights specific to China. Personality is also crucial for understanding security issues and will gain importance in the future. Personality is in the focus of some security researchers who work on the edge between information security and psychology. However, personality is specific to each individual and therefore, again, not generic enough for understanding security issues in China. Most relevant and most specific to China are cultural issues. Those issues have not been discussed up to now. Part three therefore not only offers insights that are crucial for outsourcing decisions but also opens a fundamental and exciting research field – the intersection of information security and culture.

The conclusion rounds up this thesis. It describes the broader implications of my results, sums up my findings and reveals the limitations of my work. It also presents interesting paths for further research.

During the entire thesis, I hope to find a balance between the expectations of research and practice. This thesis is a research thesis. However, it is written in a way so that practitioners should find the results useful for their actual work and can incorporate them right away. Whenever I describe research ideas on an abstract level, I sum up these ideas at the end and link them with their practical implications. After all that being said, I would like to start right away with an introduction of the basics of information security and outsourcing.

Fig. 1.5. Structure of the Thesis

Part I

Foundations

Conclusion

The Chinese Outsourcing Environment

Cultural Security Issues in China

Foundations

environment

organization

individual / group

personality

culture

human nature

2

Information Security and Outsourcing

Information security and outsourcing are two terms that are continuously floating through the news. However, they are used inconsistently which leads to different conceptions. This chapter is devoted to building the fundamentals that are required later in this thesis. It consists of definitions of the terms we will use and an introduction of the concepts behind these terms. Furthermore, I give a brief summary of the history of information security and outsourcing. I show how these topics are addressed today. With the basic understanding of information security and outsourcing that we will gain in the course of this chapter, we are well prepared for understanding and evaluating current outsourcing trends and the development of China's IT service outsourcing sector. This chapter builds a solid foundation for the rest of this thesis.[1]

2.1 Definitions

The three main terms used in this thesis are *information security, outsourcing* and *culture*. In order to work with these terms later on, it is important to create a common understanding. These terms should be defined so that we can build upon them throughout this thesis. Since culture is the most prominent and probably also the most controversial of these terms, I devoted an own section to its definition.[2] The terms and concepts behind information security and outsourcing are introduced in the following.

---

[1] Readers familiar with the concepts of information security and outsourcing can skip this chapter. However, I would like to encourage every reader to at least skim through it because it provides a new perspective, different from the common understanding.

[2] For an in-depth definition of the term culture and the concepts related to it, please see section 5.4.

2.1.1 Information Security

Information security is probably one of the most controversially discussed terms in the field of information technology. Even the previous sentence is arguably misleading because it narrows the term too much. As we will see later, information security is not only about protecting technology and technology is only one way of protecting information. Often, information is not even stored by means of any electronic medium but still needs to be secured. The term information security cannot be understood without a common definition of *information*. I define information as follows:[3]

> Information is the core of information security. It is the asset that needs to be protected. This asset can exist in various forms. Its value as an asset does not depend on its form.
> It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.[4]

If we took into account the medium and only related security efforts to electronically stored information, the term *IT security* could be used. However, since the focus lies on the asset and not on the medium, the term IT security is too narrow. It would require information technology to be the asset that is protected or the tool which is used to protect information with. Even though this limits our view, the term IT security has widely been used in the past. For broadening our understanding and highlighting the need to protect one of today's most valuable assets of a company, information, the term information security is most appropriate.

Up to now, we defined information security as the principle behind the protection of information. However, we have not clearly stated what protecting or securing information means. The traditional and most commonly accepted way of defining the security of information is by means of the CIA-triad.[5] CIA is a widely used acronym and stands for the preservation of *confidentiality*, *integrity* and *availability* of information.[6] *"Other properties such as authentic-*

---

[3] The second part of the definition is copied from ISO/IEC 17799. See ISO / IEC (2005a, p. viii)

[4] Please note that this definition of information greatly differs from other definitions. In the field of knowledge management, a distinction is drawn between data, information and knowledge. I acknowledge and embrace this difference, focusing on knowledge and how it is created, shared, retained, etc. However, for understanding information security, the distinction between those terms is not necessary. All those forms should properly be protected and information is used as a generic term.

[5] CIA, in this case, is unrelated to the Central Intelligence Agency.

[6] For definitions of confidentiality, integrity and availability, see ISO / IEC (2005b) or Committee on National Security Systems (2006).

ity, accountability, non-repudiation and reliability can also be involved"[7] but the classical CIA-triad is sufficient for this thesis.

The Business Focus of Information Security

When talking about information security and protecting information, it is important to look at it from a business point of view. All information security activities should be business-focused.[8] The main goal is to protect the information that companies need to achieve their objectives. However, protecting information by all means, without keeping the business needs in mind, can lead to an undesirable situation in which costs and trade-offs[9] of security solutions outgrow their benefits. The following quote by Whitman and Mattord highlights the demand of a business focus in information security:

> Business Needs First, Technology Needs Last.[10]

They believe that information security performs four important functions in an organization:

1. Protects the organization's ability to function
2. Enables the safe operation of applications implemented on the organization's IT systems
3. Protects the data the organization collects and uses
4. Safeguards the technology assets in use at an organization[11]

All these functions can be reduced to the goal of managing risks by trading-off money and intangibles for added security.

As I said earlier, information security is a controversial term and has often been confused with terms like computer security, network security and IT security. This confusion is due a growing scope of what people subsume under the concept of security. Those latter terms are today regarded as subsets of information security.

---

[7] See ISO / IEC (2005b, p. 2)

[8] Business-focused does not refer to a purely financial perspective but also implies paying attention to the personal needs of all stakeholders (e.g. employees and shareholders) and legal restrictions. One of the core characteristics of COBIT, an IT governance framework, is that it is *business-focused*. See IT Governance Institute (2007)

[9] The price of information security is not always counted in money but also consist of intangibles like *"time, convenience, flexibility, or privacy"*. See Schneier (2006, p. 9)

[10] See Whitman and Mattord (2003, p.43)

[11] See Whitman and Mattord (2003, p.43)

Data Security, Information Security, Business Security

In their paper *From information security to ... business security?*, Basie and Rossouw von Solms present the transformation of data security into information security. They argue that even information security should be replaced by a new term they call *business security*.

> Data security became computer security, and computer security became IT security and IT security became information security because of the better understanding of the business impact and associated risk of not properly protecting a company's electronic resources. The recent emphasis and guidelines on good corporate governance had improved and extended this understanding to such an extent that this protection must now be seen as an integral part of wider business protection, and Business Security seems to be the best term to relate the fact.
>
> Some people may reason that the term Business Security is too wide to use in this context – nevertheless, we feel that by starting to refer to Information Security as Business Security, and Information Security Governance as Business Security Governance, the role and position of protecting the electronic resources of a company will just benefit by making it a permanent item within the protection of the business as a whole, and of mediating business risks – as is required by good Corporate Governance![12]

While I agree that information security does not cover the entire spectrum of security measures a company should have in place, I disagree with their limitation to protecting *electronic resources*. As I mentioned earlier, the medium on which information is being transmitted is of no importance for its need of protection.

Since Basie and Rossouw von Solms do not define the term business security, it is hard to argue against their statement. Nevertheless, they seem to include risks like market risk and credit risk in their term business security. These risks can have an impact on the confidentiality, integrity and availability of information. They are usually even higher when services are outsourced to an external provider that suffers from one of these problems. However, these risks also pose threats to a company unrelated to its information assets and without any outsourcing relationship in place. Only if risks have a direct or indirect impact on information being processed and stored, they should be regarded as information security risks. The scope of business security is therefore too large for this thesis. Information security, as a subset of business security and not possibly being replaced by it, is the term that we will use in the following.

---

[12] See von Solms and von Solms (2005, p. 272 f.)

Security as a Process and Security as a Chain

Bruce Schneier, one of the most renowned security experts in the United States, coined two statements about information security which perfectly describe the understanding of information security that underlies this thesis. Both quotes are from his book *Secrets & Lies*.[13] The first one highlights the difference between information security and technology as a security solution:

> Security is a process, not a product.[14]

Technology alone, however advanced it might be, cannot solve security problems. Therefore, one should not buy a security solution (a product) and thereafter not care about security issues anymore. Technology can only be part of a holistic security concept. Moreover, this security concept and its successful implementation should regularly be reviewed and adapted to changing conditions and new security threats. One can therefore also speak of an information security life cycle.

The second statement by Schneier does not explain how to ensure security but rather describes the nature of information security:

> Security is a chain; it's only as secure as the weakest link.[15]

Security is often regarded as a weakest-link problem. It does not matter how strong a security mechanism is if the attacker can find another gateway into the organization that is less protected. If it is possible to bypass security barriers, they can be perfectly secure and the intruder is still able to achieve his objective. Even though the categorization of information security as a weakest-link problem is generally true, there are certain cases in which security can also be seen as a *best shot*[16] or *total effort* problem.[17] Security settings which can be described as an onion with different layers protecting its core can be seen as best shot situations. However weak these layers are, if any layer withstands the attack, the whole system is still secure. Redundancy is another example. Since availability is a state that needs to be maintained, hardware is often structured redundantly. If one hard disk fails, another seamlessly resumes its operation. If one router is not reachable anymore, the rest of the Internet still functions because one of its core design principles is redundancy. In the last category, the total effort determines the reliability of a system. *"[S]oftware validation and vulnerability testing [are tasks whose reliability] might depend on the sum of everyone's efforts."*[18]

---

[13] See Schneier (2004)

[14] See Schneier (2004, p. xxii)

[15] See Schneier (2004, p. xxii)

[16] Best shot can also be referred to as *strongest link*.

[17] I use the terms here which Hal R. Varian introduced in a slightly different context in his paper *System Reliability and Free Riding*. See Varian (2004)

[18] See Anderson, Moore, Nagaraja, and Ozment (2007, p. 631)

The concepts of security as a process and security as a chain perfectly illustrate the nature of information security beyond technical solutions.

Concluding Remarks

Information security is the art of securing information. Security managers ensure the confidentiality, integrity and availability of information that is necessary for the business to function. Therefore, they evaluate risks. Based on their risk assessment and the business needs, they develop concepts and implement security measures to protect information – a highly valuable asset for companies today. Technology is only one way of protecting information. Organizational measures play an equally important role.[19] Security concepts must be reevaluated regularly in order to adapt to changing environments. A smooth information security life cycle assures that information remains confidential, integer and always available.

2.1.2 Outsourcing

Especially in the last decade, the concept of outsourcing has been in the focus of the press. It has been widely discussed by corporations and politicians. Outsourcing has become a buzz word that stirs up extremely different feelings, depending on the cultural context. Almost everybody has an opinion towards outsourcing. It is associated with cost cutting and mass layoffs but also with advancements in information technology and incredible opportunities. Globalization is one of the first words that is mentioned in the same vein as outsourcing. China is seen as the factory of the world and India as the world's service center. However, the comprehension of outsourcing and its different forms is often rather shallow. The usage of words like *nearshoring*, *service contracting*, *service level agreements (SLA)* or *business process outsourcing (BPO)* is likely to lead to confusion.

As outsourcing is another major pillar of this thesis, I would like to create a common understanding of terminologies and concepts before exploring the field of outsourcing any further.

Definition of Outsourcing

Outsourcing can be seen as the provision of services or the production of goods by a third party. Outsourcing therefore always involves two partners – an outsourcing client and an outsourcing provider. The provider delivers a service or produces a good for its client because the client, for whatever reason, does not want to do it himself. There is a similar term called *service contracting*, which is sometimes distinguished from outsourcing.[20] The major

---

[19] For further information, see section 2.2

[20] See, for example, Axelrod (2004, p. 3)

difference is the degree of involvement. In the case of service contracting, the client is still largely involved into how the service is provided or how the good is produced. If a service is outsourced on the other hand, the client transfers most decisions to the provider. After giving initial orders, determining the way the service is delivered is part of the responsibility of the provider. Even though a line can be drawn between those two ways of providing services by third parties, the border is rather blurry. Due to this arbitrariness, I would like to keep the definition of outsourcing as open as possible. Service contracting can be seen as a form of outsourcing and for this thesis should be regarded as such. As we will see later, a strong involvement of the client is favored, usually even required, to assure a high quality service delivery. The focus of this thesis lies on the provision of services and I would like to exclude the production of goods from the definition. If only complete products are ordered and no additional service is added by the provider, *procurement* is the more suitable term.[21] Even without procurement, the field of service outsourcing is still large, as we will see in the following.

Outsourcing Services

Outsourcing is not limited to any particular type of services. It can range from infrastructure outsourcing to application outsourcing or even business process outsourcing. In this order, the integration into the client's business processes increases. Infrastructure outsourcing means that the procurement, installation and maintenance of servers and other IT infrastructure is taken care of by an external data center. Facility management is part of infrastructure outsourcing. Furthermore, even system integration services and help desk services are sometimes subsumed under infrastructure outsourcing.[22] Application outsourcing is usually defined as any kind of service related to software applications. Application development, application hosting, application maintenance, but also entire application portfolio management, are therefore part of application outsourcing. Business process outsourcing is the field in which the largest interaction with the outsourcing company is necessary. A distinction can be made between back-office services like payroll management, billing, procurement, etc. and services more visible to the employees like design and marketing or the help desk. India became famous for its provision of hotline services for many companies around the globe. Besides the services already mentioned, many other services for which special qualifications are only needed temporarily are also outsourced but do not belong to any of

---

[21] One can regard procurement as a special case of outsourcing in which there is hardly any interaction between client and provider. However, it does not fit to the scope of this thesis and is therefore excluded.

[22] Especially the latter one can also be seen as business process outsourcing.

these three groups.[23] Market intelligence, trainings or special computer foren-
sic services are only a few examples. Infrastructure outsourcing, application
outsourcing and business process outsourcing primarily cover regular tasks.
Whichever term is most appropriate depends on the types of services a com-
pany normally provides. For an insurance company, outsourcing its servers
to an external data center can be regarded as infrastructure outsourcing. For
a company that provides software as a services (SaaS), the same task would
rather be categorized as business process outsourcing because it is more central
to its core business. A company operating a data center should not outsource
its servers because server management is its core competency.

Types of Outsourcing

Besides the degree of involvement into a companies business processes, there
are various other forms of differentiating outsourcing deals.[24]

Proximity to the outsourcing provider
There are four main terms for judging the proximity to an outsourcing
provider. If a service is provided at the client's site, *onsite outsourcing* is
the right term. *Onshoring* is used for providers in the same city or same
country. *Nearshoring* is normally the selection of providers in neighbor-
ing countries or at least on the same continent. Everything else is called
offshoring. For a client in Berlin, Germany, the selection of a provider in
Munich would be called onshoring, one in Rumania is nearshoring and
outsourcing to an Indian firm is offshoring.[25] Recently, a fifth term, *global
sourcing*, gained prominence. It stands for a mixture of all forms of out-
sourcing, choosen as it seems most appropriate to a company. The delivery
of hotline services in India, application development in Rumania and the
help desk provided by a provider in the same city is an example of global
sourcing.

Number of outsourcing providers
One can differentiate between single-sourcing and multi-sourcing. If a com-
pany decides to pursue a single-sourcing strategy, one provider delivers
all services. In contrast, multi-sourcing means outsourcing to multiple
providers. Both strategies have their advantages and disadvantages de-
pending on the context.

---

[23] They can be categorized as business process outsourcing. However, the definition
of business process outsourcing should be restricted to regular business processes
which are part of a company's daily work.

[24] The following categorization is partially inspired by von Jouanne-Diedrich (2004)
(in Zarnekow, Brenner, and Grohmann (2004)) but presents the terminology used
by many researchers and practitioners in the outsourcing domain.

[25] If the Indian firm had offices in Germany and the business relationship was with
their German subsidiary, onshoring would be the more appropriate term.

Degree of outsourcing services

Services can be either insourced,[26] selectively outsourced or fully outsourced (total outsourcing).

Relationship to the outsourcing provider

Insourcing or *internal outsourcing* is outsourcing to a unit in the same company, which is distinct from the one that outsources the service. A company can also form a new entity with the outsourcing provider, a *joint venture*. If the client is outsourcing to an external provider, this form is called *external outsourcing*.

All these terms are not fixed and many practitioners and researchers use other terms or use the terms differently. I tried to select the most commonly used terms and the their common meanings. Besides those terms, there are many more possible ways of describing special kinds of outsourcing. This list is not meant to be exhaustive. It should rather provide a first overview of terms that one is likely to encounter.

Advantages and Disadvantages of Outsourcing

Outsourcing has recently become a large-scale phenomenon. The trend was started by large insurance companies and financial institutions. They wanted to cut their expenses and concentrate on their core business. An own highly-skilled IT department for each branch office was unreasonable. Therefore, they consolidated their infrastructure and personnel and in the end outsourced it to external providers. Those providers could deliver the same service with a higher quality for less money. Today, outsourcing of IT services is not limited to multinational enterprises or knowledge-intense industries anymore. Even small and medium enterprises (SME) start realizing the advantages of outsourcing,[27] for very similar reasons as their large counterparts. However, there are also risks related to outsourcing. In the following, I would like to give a brief overview of advantages and disadvantages or rather opportunities and threats of outsourcing.

There are three main reasons for outsourcing: *cutting and restructuring costs*, *streamlining the organization* and *the provision of higher quality services*. By outsourcing IT services to another company that is specialized in this field, a company can optimize its expenses in two major ways. It can cut costs because the external provider is able to provide the same service at a lower cost. This is mostly due to economies of scale. Since this provider serves many clients at the same time, it can purchase hardware cheaper by bundling

---

[26] Insourcing is a special case. It usually means outsourcing a service to an internal unit with is normally independent of the unit that outsourced the service.

[27] In the past, SMEs already outsourced many services to other companies in their own region, simply because they could not provide the services themselves. The major shift that is happening today is that even offshore outsourcing is starting to take off amongst SMEs.

orders, personnel is used more efficiently, etc. The second cost advantage is that a company can restructure its costs. It can convert variable costs into fixed costs. This improves the managements ability to budget and oversee expenses. Another advantage is that an organization can be streamlined by outsourcing services. It can concentrate on its core business and does not need to care about back office services anymore. Finding and training staff, especially in the IT domain, is cumbersome and distracts from the main business. Furthermore, outsourcing a limited set of services can start an impulse for the entire organization to change. These two reasons, the cost advantage and a more streamlined organization,[28] would probably be enough to convince companies of outsourcing as an opportunity. However, in addition to these two advantages, outsourcing services can lead to an increase in service quality. An outsourcing provider should have better skilled personnel and more experience with the desired services because the provision of these services is its core business. This experience is gained by more specialized staff and working for many clients at the same time. Therefore, the provider can also react to new demands faster and more easily. This reduces the time to implement new ideas. In the end, outsourcing can even reduce risks because of two reasons. The provider can better manage the risks because of the advantage in knowledge and experience and a client can demand a certain service quality based on contractual agreements (Service Level Agreements).

Despite all those advantages, the decision to outsource is extremely complex. It involves many risks that need to be evaluated properly.[29] Especially companies inexperienced with outsourcing do not properly manage risks even though that can have lethal consequences. The broad spectrum of risks is often surprising to them. Two major risks are hidden costs and the dependency on the outsourcing provider. In addition, there are security risks because the operations and performance of the provider is harder to control than the one of the own IT department. Those risks can be considered part of the second category. However, since they are the main focus of this thesis, they should be regarded as a category on their own. Hidden costs can be transaction costs that were not anticipated. Selection of and negotiation with the outsourcing provider, transition of all services and downsizing of own staff and technology, contract and relationship management as well as controlling of the providers performance all require efforts and money that is often underestimated. An opportunistic provider can raise prices as soon as the client is locked in. That is one of the reasons why companies often depend on their providers to a large extent. They dismiss employees and dispose infrastructure because they do not seem necessary anymore and costs can be lowered. It is also likely

---

[28] I assume that the services are provided at least at the same level of quality by the external provider.

[29] Basic introductions to outsourcing risks and risk evaluation are offered by Aubert, Patry, and Rivard (1998) and Aubert, Dussault, Patry, and Rivard (1999).

that highly skilled employees will leave a company that outsourced most of its IT services because they do not see any career perspectives or might even be afraid to get laid off in the future. Thereby, important knowledge is lost that is necessary to cultivate and supervise the outsourcing relationship. This lock-in is a substantial problem if the outsourcing provider gets into serious trouble and cannot provide the services anymore. In the worst case, if the provider for example files for bankruptcy or is hit by a natural disaster, this might result in the services being unavailable without any prior warning. This is a serious security risk for the outsourcing client. With services and data being unavailable, maybe even irrecoverably, the client might not be able to function anymore if it strongly relies on the outsourcing provider. There are many other security risks. However, I will not address those here. This thesis focuses on security risks in outsourcing relationships and provides examples of these risks in many other chapters. The three categories discussed do not cover all kinds of risks related to outsourcing. There are other risks like the possibility of an image loss if a company outsources jobs to offshore locations,[30] just to name an example. However, those three categories – hidden costs, dependability on the outsourcing provider and security risks – are the three major risks that companies need to manage.

The decisions of whether or not to outsource but also the provider selection are highly important. Companies planning to outsource should follow a well-defined process, weighting opportunities and risks, also considering indirect effects for example on the morale of the own employees, and scrutinize the background of potential partners. The selection of an IT service provider must not be seen as renting a few servers but rather as hiring an entire IT department. The relationship therefore needs to be cultivated continuously after the initial selection. This change in mindset reduces the risks and is more likely to lead to the desired outcome.

Concluding Remarks

In this section, outsourcing has been defined as the provision of services, regardless of the outsourcing destination or the degree of client involvement. This description of the concept of outsourcing, as well as its opportunities and risks, cannot be exhaustive.[31] This thesis is not an introduction to outsourcing or a discussion of certain aspects of outsourcing but an analysis of the

---

[30] This is often regarded as unsocial and unpatriotic behavior because the company does not fulfill its social obligation. The effect largely depends on the services a company provides. In consumer goods, this is more likely to affect the company than if they only provide services for other businesses. There are many other direct and indirect risks.

[31] For more detailed information, please refer to the respective literature. For example: Lacity and Hirschheim (1993); Stees (1998); Lacity and Willcocks (2001); Axelrod (2004); Brown and Wilson (2005); Hirschheim, Heinzl, and Dibbern (2006); Carmel and Tjia (2006). German readers, see also Amberg and Wiener

influence of culture on information security. Outsourcing IT services in China is its scope. The description above ensures a common understanding of the terminology used and sensitizes for common mistakes, especially deficiencies in risk management. Information security risks are a serious threat to companies that is often underestimated. Outsourcing offers promising opportunities if the risks are managed properly.

2.1.3 Intersections of Information Security and Outsourcing

This thesis focuses on information security risks related to outsourcing of IT services in China. Recognizing and understanding these risks can seriously alter outsourcing decisions. In order to clarify the relation between what C. Warren Axelrod calls *"the two most dynamic, difficult, and controversial areas of information technology today, namely, outsourcing and security"*,[32] I will present all intersections of these two areas in a two-by-two table. Axelrod introduced this matrix in his book *Outsourcing Information Security*.[33]

	The Outsourcing	The Security
. . . of Outsourcing	Subcontracted IT Services	Secure IT Services
. . . of Security	Subcontracted Security Services	Secure Security Services

Table 2.1. The Intersections of Outsourcing and Security

By reviewing each of the possible intersections, we will understand its importance for this analysis.

The Outsourcing of Outsourcing – Subcontracted IT Services

This intersection refers to the case in which outsourcing providers subcontract IT services to other outsourcing providers. Even though this is not the main focus of this thesis, it is a business strategy that outsourcing providers might choose. Their customers need to be aware of this option and agree with their outsourcing providers on specific terms concerning third parties providing services for them. This is particularly relevant if there are legal requirements imposed on the company that would like to outsource its IT services.

(2006); Söbbing (2006). Standards like BSI (2005) and BITS (2003) provide further advice on how to manage security risks.

[32] See Axelrod (2004, p. xx)

[33] See table 2.1 as in Axelrod (2004, p. xxi)

The Security of Security – Secure Security Services

The *security of security* is about checking if security technologies (e.g. firewalls), security service providers (consultants, managed security service providers, etc.) or own security personnel might pose new security threats on the organization. While background checks on security staff and a careful selection as well as reevaluation of security technologies are highly important to mitigate security risks, this issue is not the main focus of this thesis. There is no direct relation to outsourcing of IT services. Organizations need to make sure that their outsourcing providers stick to their requirements but the way in which their providers evaluate those risks will not be discussed.

The Outsourcing of Security – Subcontracted Security Services

As a special case of outsourcing, some companies outsource information security services to external providers. Common outsourced services include the physical protection of the site (e.g. security guards and alarm systems), intrusion detection, monitoring and forensics. The main reasons for outsourcing these services are cost-cutting and the concentration on core competencies which leads to the need for external expertise to provide high-quality services. During my research, I found that these services were normally outsourced as part of bigger projects. Hardly any company chose the special case only to outsource security service but rather outsourced them along with their entire IT operations. I will therefore focus on the bigger picture and regard outsourced security services as part of outsourcing projects.

The Security of Outsourcing – Secure IT Services

The *security of outsourcing* represents a particular view on outsourcing projects. Another possible view would be a discussion of financial aspects of outsourcing projects. In this thesis, the security of outsourcing is the main topic. It includes an analysis of potential security risks while outsourcing IT services in China and proposes ways of mitigating them. As we will see later, security issues can occur during the entire outsourcing life cycle and risk management should therefore be an ongoing effort in all companies that outsource IT services. Potential risks are numerous. They can be technological, organizational, legal, cultural, etc. It is therefore highly important for the success of an outsourcing relationship to promote a broad view on information security, beyond technological risks.

Outsourced security services and subcontracted IT services represent special cases of outsourcing that managers should keep in mind. They require particular supervision. Secure security services are simply a mean to reach the end – secure IT services. How to ensure a high level of security while outsourcing IT services in and to China, the security of outsourcing, is the main topic of this thesis.

2.2 The Evolution of Information Security

When asked for security threats, most people talk about *viruses* and *spam*. More technology savvy people think of *trojan horses* and *buffer overflows*. Hackers are seen as intruders who pick a target and try to get into a company's network. They hack for their own monetary benefit or work as industrial spies. Some might be patriotic techies trying to disclose industry or state secrets, maybe even working for their governments. Or some others just hack for fun and acknowledgement, proving their skills to themselves and to the community. However their motivation, hackers are regarded as outsiders – people working for another company, another government or just for themselves. They try to get into computer systems and have to circumvent security measures for doing so. Therefore, companies and also individuals have to build a shell around their computer systems in order to keep these evil-doers out. Firewalls are the most common security measure. To say it in Gurpreet Dhillon's words:

> The concern [...] has been on maintaining a security perimeter around information processing activities.[34]

He wrote this in 1995 and already then realized that the concept of perimeter firewalls is a concept of the past. This concept is built on a wrong assumption that needs to be rectified: *Hackers are outsiders. As outsiders, they can be kept out of the network*. While it is true that some hackers are outsiders, a large share of attacks comes from people within the organization. Accepting that attackers might be within the organization already, one realizes that they cannot be kept out of the network. They do not have to circumvent any security measures anymore. In those cases, a perimeter firewall does not work. In addition, there is another development that challenges those assumptions, the transformation of organizations.

2.2.1 Decentralization of Structures

Perimeter firewalls have provided sufficient protection as long as organizations and their IT infrastructure were centrally organized. However, organizations are in a transformation process. Due to a rapid decline of communication costs, the structure of organizations changes.[35] Decision making but also IT infrastructure is increasingly decentralized. Technological advancements allow devices to become smaller and employees are expected to be mobile like never before. Especially knowledge workers can work from anywhere. They can work from the headquarter, a subsidiary, at home, from a hotel, a cafe or even anywhere in between (e.g. at an airport or on a train). In order to fulfill their jobs,

---

[34] See Dhillon (1995, p. 43)

[35] For a more detailed description of this process, see page 37, focusing on work by Thomas W. Malone.

they have to be able to access corporate data from anywhere. Besides the own employees, many other stakeholders also need to access data. Another effect of declining communication costs is the steep increase in interaction between companies, their suppliers and partners. Just-in-time production requires a continuous exchange of information. Furthermore, companies outsource services to providers around the globe for various reasons. Those services are not only special services outside of the day-to-day operation. Companies start to outsource integral parts of their operations without which they would not be able to function anymore. Therefore, besides the regional also the institutional borders of the entities sharing data are vanishing. The traditional concept of the perimeter is not sufficient anymore.

2.2.2 Institutionalization of Information Security

In order to react to those changes, there is a new approach to information security. Besides technical measures, companies start focusing more and more on organizational measures. A modern security concept includes security policies that tell employees and partnering companies how they should behave.[36] However, the concept of security policies itself leaves a few open problems. Employees need to read and understand them. Even if they know how they should behave, they act differently because the policies are too cumbersome or conflict with their own goals. Therefore, security managers need to find a way to enforce those policies. Punishment is one possible solution. However, since employees are increasingly mobile, their behavior is hard to supervise. The best solution would be if employees would stick to the policies by themselves. Therefore, security awareness campaigns and trainings are on the agenda of many security managers. They sensitize employees for the topic and ideally create a security culture within the firm. If a security culture is built, positive values towards the establishment and maintenance of a high level of information security are established in the minds of all employees. Furthermore, social pressure is established because social norms demand secure behavior. This is an important step towards a more secure environment in changing organizational structures. However, if employees are traveling alone, the social pressure is inexistent. Partners and outsourcing providers are hardly affected by a company's security culture because the exchange of employees is too sparse. There are two possible solutions for solving these issues. I would like to touch on both of them in the following.[37]

---

[36] Besides security policies, there are service level agreements with providers that define certain security requirements.

[37] For a more detailed description of new challenges and the deficiency of current security concepts, see this article in German: Glaser and Pallas (2008)

2.2.3 Two Possible Solutions

In order to cope with the challenges mentioned above, I see two possible solutions: *Knowledgeable Selection* and *Economic Incentives*. Company need to understand their employees (and future employees) and partners. It is not necessary that they only recruit employees and select partners that completely fit to the own corporate and security culture. It is more important to understand their behavior so that security concepts can be modeled around it. If a company anticipates certain threats, security measures reduce their likelihood or lower their impact if they cannot be prevented. In order to understand behavior in the field of information security, there are two main disciplines in which research is conducted: *Economics* and *Psychology*. In order to understand the behavior of groups, a third field should be added – *Sociology and Cultural Studies*.[38] Sociology and cultural studies go beyond explaining the behavior of individuals. Whereas economics strives to find universal rules and psychology is directed toward the individual, those two disciplines are especially helpful for understanding the behavior of groups. Their insights can be used to examine the own organization but more importantly for scrutinizing new employees and partners (e.g. outsourcing providers). By predicting security threats based on the behavior of employees and partners, companies can reduce the risk before security incidents occur. The second solution, aligning the incentives of employees and partners with the ones of the own company is a very new field of study as well. If the incentives are aligned, there is no need to control behavior anymore. Employees and partners already act in the best interest of the company.[39] I believe that these two solutions are highly interlinked. If one does not understand group processes and cultural character traits, it is difficult to set incentives. People in different cultures have different goals. Just understanding behavior and trying to circumvent all possible threats by technical and organizational countermeasures is unlikely to lead to desired results. Security measures can never cover all possible scenarios and demand a lot of supervision. A mixture of both approaches is necessary to achieve the desired outcome.

In the past, technical and organizational countermeasures could assure an adequate level of security. Today, with international workforces and highly interlinked business relations these measures cannot be employed without a proper understanding of human behavior. By combining theories from the fields of economics, psychology, sociology and cultural studies, we can start to understand behavior and put suitable security measures in place. By setting incentives and thereby aligning the interest of employees and partnering organizations with the needs of the own company, we can minimize security risks in this new environment.

---

[38] See also section 5.1
[39] Frank Pallas conducts extensive research in this field.

2.3 The History of Outsourcing

> It is the maxim of every prudent master of a family never to attempt
> to make at home what it will cost him more to make than to buy.
> The taylor does not attempt to make his own shoes, but buys them
> of the shoemaker. The shoemaker does not attempt to make his own
> clothes, but employs a taylor. The farmer attempts to make neither
> the one nor the other, but employs those different artificers.[40]

Outsourcing the provision of services and the production of goods to third
parties is not a new phenomenon. On the contrary, it was always present
throughout history. By looking at its development over centuries, one can
capture underlying schemes which help to classify and understand upcoming
trends. Advances in information and telecommunication technology enable
new forms of cooperation that foster radical changes in the business world. In
order to broaden our view, we should start with a short historical retrospect
and an introduction to the economics of outsourcing.

2.3.1 Tradition and Economics of Outsourcing

Even the traditional division of labour in hunter-gatherer societies can be seen
as an early form of outsourcing. While men typically went hunting, women
gathered wild fruits and vegetables. Each group contributed an important
share to the nourishment of the other group, or rather the society as a whole,
by fulfilling the task that was most appropriate to their learned and inherited
skill set.[41]

But why is Smith's statement not just a claim, a hypothesis, but an eco-
nomic principle that has been present since the early days of mankind? From
an economic perspective, the explanation is evident: If we consider only two
goods, just to simplify, *"the opportunity cost[42] of one good is the inverse of
the opportunity cost of the other. [...] Unless two people have exactly the same*

---

[40] See Smith (1776, book 4, chapter 2)

[41] One might argue that this cannot be seen as a form of outsourcing because both
men and women are part of one economic and social unit. Therefore, specializing
on different tasks would be pure division of labour and not outsourcing since no
external party provided a service or a product to the community. However, this is
merely a matter of perspective. If one regards all men as members of an individual
group, they outsourced the task of gathering, which they would normally have
fulfilled themselves, to another entity, the group of women. The same is true if we
see one individual human as a single entity. By narrowing the scope and therefore
reducing the number of people within a economic and social entity, any kind of
cooperation can be seen as a form of outsourcing because it implies the exchange
of services and products between different entities.

[42] *opportunity cost:* whatever must be given up to obtain some item, see
(Mankiw and Taylor, 2006, p. 815)

opportunity cost, one person will have a comparative advantage[43] *in one good, and the other will have a comparative advantage in the other good."*[44] Due to those comparative advantages, people always specialized in what they can do best, whereas best means with the lowest opportunity costs. Trade as well as the provision of services for other parties has always been beneficial for the individual and the society as a whole.[45]

Today, this economic principle is extremely present in the media and management books. It is pronounced in lax ways as: *Do what you can do best, outsource the rest.* Or a bit less striking: *Concentrate on your core competencies.*

2.3.2 The Cost of Outsourcing

Focussing on the pure economic rationale behind outsourcing decisions, and therefore leaving other reasons aside,[46] decision makers have to consider two kinds of expenses of outsourcing projects: production costs and transaction costs[47]

Malone, Yates and Benjamin argued already in 1987 that the emergence of electronic interconnection and the more intense use of information technology reduces transaction costs faster than production costs. The reduction of transaction costs leads to a shift from hierarchies to markets, as ways of coordinating economic activity. As a consequence, the growing use of information systems makes outsourcing more beneficial than internal production.[48]

While it is obvious that offshoring production and service delivery to low wage countries is likely to reduce production costs, transaction costs rise. Due diligence of potential partners,[49] working in a foreign legal setting, another cultural environment, etc. is more costly (directly and indirectly) than in

---

[43] *comparative advantage:* the comparison among producers of a good according to their opportunity cost, see (Mankiw and Taylor, 2006, p. 815)

[44] See Mankiw and Taylor (2006)

[45] *"Trade is never a zero-sum game; it profits buyers and sellers alike. It depends for its benefits not on competitive advantage, but on comparative advantage, a crucial distinction."* See The Economist (2003)

[46] Political reasons, for example, often play an important role in outsourcing decisions. Other reasons include: focusing on core business, improving performance and reliability, increasing flexibility, etc.

[47] *"Production costs include the physical or other primary processes necessary to create and distribute the goods or services being produced. Coordination costs include the transaction (or governance) costs of all the information processing necessary to coordinate the work of people and machines that perform the primary processes."* See (Malone, Yates, and Benjamin, 1987, p. 485)

[48] See Malone et al. (1987)

[49] Language barriers, lack of standard processes and certifications as well as problems concerning background screening and evaluation of the outsourcing provider's staff, just to name a few, raise the uncertainty that clients face and make due diligence extremely hard. Opportunistic behavior of outsourcing providers can turn the outsourcing market into a market for lemons.

the home country. The fall of coordination costs, as a result of the rise of information technology, is a major reason behind the trend towards offshore outsourcing. Production and service delivery are increasingly outsourced to offshore locations because of lower labor costs and falling coordination costs.

2.3.3 A Brief History of Recent IT Outsourcing

The introduction of electronic data processing systems in the mid-twentieth century and global communication through computer networks started a new era of outsourcing.[50] By means of electronic data exchange, communication costs have dramatically declined. The results of outsourced tasks can be made available immediately after their completion. No physical documents have to be shipped anymore.

The modern outsourcing era started as early as 1962, with the foundation of Electronic Data Systems (EDS) in Texas. EDS was founded by Ross Perot, a former IBM employee, with the idea to provide computing power to other enterprises.[51] Outsourcing the provision of IT services was not a choice for most companies that wanted to use IT systems at that time. Due to the high price of IT hardware and the lack of IT professionals, they simply could not afford to build own computing centers and had to use computing power provided by third parties.[52] In 1963, EDS signed a five-year facility management agreement with Frito-Lay that can be seen as a breakthrough in the outsourcing industry. It started a shift from hourly paid short-term deals to long-term partnerships between outsourcing providers and their clients. Even today, EDS is still one of the leading IT Outsourcing and Business Process Outsourcing providers worldwide.

Until the early 1970s, when minicomputers became popular and replaced large mainframes, time-sharing was the dominant model of using computing power. Only new developments in the computer architecture made the operation of own computer systems affordable to single companies and even departments.[53] Outsourcing became a choice instead of a necessity. This choice was even strengthened by the rise of personal computers in the early 1980s.

The next milestone in the recent history of outsourcing was in 1989, when Eastman Kodak *"announced their outsourcing contracts with IBM, Business-land and DEC".*[54] It included the operation of Kodak's data centers and the support of its PCs for a period of 10 years, worth 250 million USD.[55] Kodak was not the only firm to outsource its IT operations at that time. Amongst others, all signing multi-million dollar deals, were American Bankshares, Enron

---

[50] See Axelrod (2004, p. 181)
[51] See Electronic Data Systems (2007) and Mason (1990)
[52] See Axelrod (2004, p. 181)
[53] See Axelrod (2004, p. 186)
[54] See Lacity and Hirschheim (1993, p. ix)
[55] See Axelrod (2004, p. 186)

and Continental.[56] Research by Marc Lacity and Rudy Hirschheim suggests that the rise of outsourcing was not due to any new ideas concerning the provision of IT services by external providers but rather based on the symbolic power that the outsourcing deals with prominent American corporations had on the rest of the industry.

In the late 1990s, the next big wave of outsourcing started. In contrast to the preceding waves, this wave did not focus on the operation of computer systems but on software development and maintenance. This trend was initiated by two main events. First, the US American *Telecommunications Act of 1996*[57] opened the telecommunications market and new operators spread. Since the need for bandwidth doubled every three months for about two years, operators predicted that this trend would continue and heavily invested in their telecommunication infrastructure. Due to the dot-com bubble, there was enough capital, even for newly founded companies, to build own networks. These companies mainly built long-distance fiber optic cables around the world. As a result of wrong predictions, there was an immense overcapacity and even long-distance communication became basically free.[58] India was linked with the United States without having invested into own telecommunication infrastructure. The second event was that the year 2000 approached. US American companies feared that their computer systems might crash and did not have the resources to fix them. Since telecommunication with India was almost free and India had a large pool of programmers, Indian workers were the ones fixing American software. That was the start of the Indian outsourcing dream.[59]

At almost the same time, in the year 2001, China joined the World Trade Organization which boosted the number of companies moving their production offshore to China.[60] Even though China became most known for being the world's factory, it also started turning into India's fiercest competitor, offering high-quality IT services. China's target to surpass India becomes apparent in its *1000-100-10 project* which is part of its 11th five-year plan. The project's goal is to select 10 cities as outsourcing bases. 100 multinational corporations shall obtain IT services from 1000 newly started Chinese outsourcing providers.[61]

In section 3.2, I lie out possible paths for China's and India's role in the IT service outsourcing market in 2012.[62] However the outcome, both countries will continue to enlarge their outsourcing business and China is very likely to

---

[56] See Lacity and Hirschheim (1993, p. 1)

[57] See Federal Communications Commission (1996)

[58] See Friedman (2005, p. 66 ff.)

[59] See Friedman (2005, p. 103 ff.)

[60] See Brahm (2002)

[61] See Ministry of Commerce, People's Republic of China (2006)

[62] This scenario description is based on Popkin and Iyengar (2007). Their methodology is inspired by Schwartz (1996).

become another dominant player in the outsourcing market in the upcoming years.

2.3.4 Changes in Societies and Corporations

After having analyzed recent single events leading to shifts in the outsourcing market, the development of outsourcing needs to be put into a broader contextual framework. Thomas W. Malone compares developments in business – outsourcing and market-like coordination within firms in particular – to the development of societies. In his opinion both developments are based on the same underlying reason, the fall of communication costs.[63]

Going back to hunter-gatherer societies, they mainly consisted of small independent groups of people called bands. When communication costs decreased because humans invented the technology of writing, hierarchical coordination became possible and bands united to make use of economic and military advantages over smaller groups – kingdoms formed.[64] Johannes Gutenberg further cut communication costs by inventing movable type printing in the 15th century. Citizens were therefore better informed and could make their voices heard in the public debate. The possibility for groups, other than the ruling government, to express their ideas was the beginning of a new form of coordination – democracies.[65] The participation of individual citizens is even intensified today by means of electronic communication. Weblogs, video sharing websites, etc. make it possible for anyone to express his or her opinion. Wikis, mailing lists, etc. enable groups to coordinate political activities without the need for any formal entity like a party or lobbying organization.[66]

The same process that societies went through – from small independent entities, to large hierarchical organization, to networked webs[67] – is taking place in the business world. One of the earliest forms of economic units were

---

[63] See Malone (2004)

[64] Decentralized coordination was not possible because communication was primarily one-way and getting all citizens together to discuss important issues was basically too expensive.

[65] It can be argued that first democracies started a lot earlier. However, *[t]he early democracies of Athens and Sparta were confined to small states, and were based on a slave population without civic rights. There was not even a conception that slaves might or should take part in politics, and the slaves vastly outnumbered the citizens.* (Clayton, 1911) Furthermore, as Athens and Sparta covered relatively small areas, communication was a lot easier than in large nations.

[66] In countries without freedom of speech and freedom of the press, these technologies can be used to express ideas and to start grassroots movements to turn their political systems into democracies. Currently, governments have immense problems filtering the blogosphere, especially if their citizens come up with creative ideas how to replace forbidden words with unambiguous but concealed expressions.

[67] See figure 2.1

Fig. 2.1. The Development of Societies and Businesses

small family businesses. New telecommunication and transportation technologies made it possible to build large, hierarchically coordinated enterprises. Despite current headlines presenting endless mergers and acquisitions, research, that was conducted in the mid-1990s by Brynjolfsson, Malone, Gurbaxani and Kambil, shows that the average size of U.S. businesses is declining.[68] According to Malone, a major reason for that development is outsourcing, reinforced by new communication technologies.[69] In the 1960, when the Xerox machine became popular, not only 1-to-1 or 1-to-a-few but 1-to-many communication became possible. Thirty years later, 1-to-many but also many-to-many communication exploded with technologies like e-mail, conference calls and the Web as well as platforms like Wikis, social networks, etc. running on top of it.[70] By making use of these technologies, corporations have started to cooperate more intensively and to form business webs. These webs can either be decentralized, a working coalition in which each partner uses resources of the others, or centered around one company.

An example of the latter is the ecosystem that has developed around Apple.[71] In June 2007, Business Week ran a story titled *Welcome to Planet Apple*, in which it quotes Apple's CEO Steve Jobs saying *"Apple lives in an ecosystem, and it needs help from other partners."* At that time, more than 200,000 companies had created Apple-compatible products which were necessary to drive the success of Apple's own software and hardware. Today, it seems self-evident that Apple does not develop its hardware components itself. Research and the production of processors, displays, batteries, etc. is all outsourced to other companies. Amongst its partners are firms like Intel, AT&T, YouTube, Starbucks, Google, TNT and even Microsoft. Apple even signed deals with all major movie studios to include their movies into its video rental service. Apple calls them partners, but in the end, those companies can also be seen as

---

[68] See Brynjolfsson, Malone, Gurbaxani, and Kambil (1994)

[69] See Malone (2004, p. 31)

[70] See Malone (2004, p. 33)

[71] Dell is another excellent example vividly described by Thomas Friedman in his book *The World is Flat.* See Friedman (2005, p. 414 ff.)

Apple's outsourcing providers. They provide services and products for Apple which Apple combines to create own products. Apple's job is the one of a composer. It takes resources and organizes them in a new way – something we might call *mashup* today. It further is in the role of a conductor, making sure that research, marketing, production, shipping as well as service and support are all smoothly integrated.[72]

By using information technology, the integration of partners, or outsourcing providers, into the own organization becomes easier and controllable. Corporate borders blur and a business web is created. Technology has been the boost for outsourcing and cooperation.

2.3.5 Concluding Remarks

Outsourcing, even to offshore destinations, is not a new development but has existed since the early days of mankind. However, recent advancements in information and communication technology have lifted its relevance to an unprecedented level.

Outsourcing and the cooperation of companies in form of business webs let borders between these firms blur and almost vanish. Modern supply chain management requires companies to continuously exchange information with their suppliers. Outsourcing payroll and accounting tasks to other firms requires companies to transfer highly sensitive information via data channels. Since borders between firms blur, traditional security concepts (like perimeter firewalls) are not sufficient anymore. New concepts for securing information need to be developed by research institutes and corporations. This is even more urgent because even today many outsourcing providers operate in other countries. Due diligence is hard to conduct because of the distance but also due to cultural differences whose impact can hardly be anticipated. Operating in different jurisdictions even rises the complexity.

Outsourcing can be seen as a flattener of commerce, fostering entrepreneurship around the world. It offers an incredible opportunity for large corporations and small companies alike. However, the risks of this new form of global outsourcing need to be addressed as well.

2.4 The Outsourcing Process

As we saw, the reasons behind a company's outsourcing decision might differ and there are numerous variations of outsourcing deals (in scope and focus). However, there is a set of tasks that each company that would like to outsource

---

[72] Trends like the rise of web services enable companies to earn money by conducting their interaction. By making use of concepts like *Software as a Service* companies can start highly scalable business models. If they integrate services like *Amazon S3* and *EC2*, these companies do not even need to set up their own data centers.

services to another provider needs to go through. The depth in which each step is being dealt with depends on the individual situation of each company. Nevertheless, the overall pattern is largely similar for all kinds of outsourcing activities and can be described as the *outsourcing process.*

The main reason why companies should go through a well-defined outsourcing process is to ensure the success of their outsourcing deals. Success can be measured in numerous ways that vary due to differences in business needs and outsourcing goals. I see the success of an outsourcing deal as a high correlation between expectations and outcome of the deal without any surprises that got a negative impact on the customer. Minimizing the gap between expectations and the actual outcome of an outsourcing activity means reducing or rather managing potential risks. Many of the steps taken before, during and after outsourcing services to an external provider are therefore aimed at the minimization of risks. Not all but a large share of these outsourcing risks are security-related.

In the following, I will present three outsourcing process frameworks that are applied and suggested by different organizations. Since these organizations each got their own agenda, their individual goals and their business focus might be incorporated in their process models. If that is the case, I will highlight it. The first model that I present was developed by the management consultancy *Boston Consulting Group.* Looking at it in depth, it presents all major steps of the outsourcing process. However, the focus of its model is biased by its corporate interest, as we will see later. To deepen the understanding of security issues in outsourcing processes, the next model presented is by the *German Federal Office for Information Security (BSI).* It shows that security issues are part of every single step of the outsourcing cycle. Since the BSI did not develop the entire publication itself but cooperated with security experts, practical experience is incorporated into the model. Looking from a practitioner's point of view, we will be able to observe in which areas those experts expect security risks and how they propose them to be handled. The last model presented is from the field of academia and should therefore provide the most independent view on the outsourcing process. It is neither biased by corporate interests nor has a specific focus on the outsourcing process. Furthermore, it clusters potential security risks in a three layer model which I will later use for structuring the presentation of my findings.

2.4.1 A Consultancy's Outsourcing Life Cycle

The Boston Consulting Group (BCG) developed an own outsourcing framework, its outsourcing life cycle, that is mainly based on its outsourcing experience in the financial sector.[73] It consists of the following six steps:

1. Strategy

---

[73] See Boston Consulting Group (2005, p. 13 f.)

Fig. 2.2. BCG's Outsourcing Life Cycle

2. Selection
3. Negotiation
4. Transformation
5. Contract and Relationship Management
6. Reevaluation

Out of these six steps, BCG believes that getting the outsourcing strategy right is most crucial because it lies the foundation for all further activities. This includes *"defining a possible outsourcing scope"*, *"reviewing all IT processes"*, *"considering [your] potential of optimizing them without outsourcing"*, *"determining [your] readiness to seek outsourcing solutions according to strict organizational and cultural requirements"* as well as *"setting priorities"* by ranking IT processes according to their outsourcing potential.[74] BCG's experts make one very interesting remark that highlights problems that outsourcers experienced in the past. An organization should only outsource well-understood and well-controlled processes. They believe that it is almost impossible to solve internal problems by outsourcing problematic processes.

Comparing BCG's suggestions to those of one of its strongest competitors, McKinsey & Company, one easily notices similarities. McKinsey also focuses on the beginning of the outsourcing process, the steps that BCG calls *strategy* and *selection*.[75] In their opinion, the most important steps are *"identifying IT activities that can be moved offshored"*, *"defining the right model to adopt (i.e., in house captive or outsourced)"*, *"choosing the right location(s)"*, *"se-*

---

[74] See Boston Consulting Group (2005, p. 13)

[75] McKinsey's presented five-step methodology is based on an article on IT offshoring but should be applicable to any other outsourcing activity as well.

lecting the right vendor (if outsourced)" and *"determining the appropriate implementation sequencing".*[76]

Both companies, BCG and McKinsey, focus on the beginning of the outsourcing process, defining a strategy for choosing the right outsourcing scope and model. Even though these certainly are highly important steps, their preference seems to be linked to their consulting services. As strategy consulting firms, their focus lies on strategy definition rather than supporting their clients during the outsourcing negotiation, the actual outsourcing implementation and the management of the outsourcing relationship.

Due to this business-related bias emerging in frameworks developed by individual firms, we need to take another perspective. In the following, we will look at frameworks developed by rather independent organizations.

2.4.2 BSI Baseline Protection Manual and BITS Framework

The *German Federal Office for Information Security (BSI)* is the IT security service provider of the German government. In this role, it does not only provide services for public authorities but also conducts security research, develops standards and educates citizens as well as small and medium-sized enterprises about information security issues.

Whereas the former framework developed by the Boston Consulting Group seems to focus on issues supporting its corporate interests, all documents developed by the BSI, as an independent agency, were reviewed by various stakeholders and mutually agreed upon so that they should follow a rather holistic approach.[77] In contrast to BCG's outsourcing life cycle, documents by the BSI focus on information security issues. For an outsourcing framework, reviewing it on an abstract level, it does not make a difference whether the framework addresses corporate management or information security managers. Information security issues play an important role in all phases of an outsourcing process so that all phases of the process are introduced.

The BSI developed an overall information security manual which is called *IT Baseline Protection Manual* or *IT-Grundschutz Catalogues.*[78] *"The objective of these IT-Grundschutz recommendations is to achieve a security level for IT systems which is reasonable and adequate to satisfy normal protection requirements and which can also serve as the basis for IT systems and ap-*

---

[76] See Ip, Hodges, and Ho (2003, p. 108 ff)

[77] The fact that most BSI publications were co-written by information security professionals, often working for information security consultancies, might countervail the publications' independence. To ensure the absence of corporate influence, publications are always reviewed. Therefore, working on the BSI publications is rather being seen as a marketing tool by many information security professionals.

[78] The IT Baseline Protection Manual is reviewed and updated every six months and published on the website of the BSI. See BSI (2005) and `http://www.bsi.de/english/`

plications requiring a high degree of protection."[79] It is mainly directed at small and medium-sized enterprises but provides valuable insights and advice for large corporations as well. One component of the IT Baseline Protection Manual is a section on security issues related to outsourcing activities.[80] This section includes a summary of all important phases of an outsourcing partnership which are listed in the following:

1. Strategic planning of the outsourcing project
2. Definition of the essential security requirements
3. Selection of the outsourcing service provider
4. Form of contract
5. Preparation of an IT security policy for the outsourced IT assets
6. Migration phase
7. Planning and safeguarding ongoing operations

The purpose of the BSI publication is to reduce security risks related to outsourcing activities of a company. A similar document was developed by the *BITS Financial Services Round Table*, the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships*.[81] It provides an in-depth description of the individual outsourcing phases, highlights potential risks and proposes approaches to manage those risks.

Comparing the frameworks by consulting firms with those authored by independent organizations, we notice a difference in focus, due to different interests of the stakeholders. While consulting firms might want to sell their services and see their core competencies in the early phases of outsourcing deals, namely strategy development and provider selection, the independent frameworks, focusing on risk management issues, cover the entire outsourcing life cycle. Even though the second kind of frameworks we looked at are more focused in their purpose (reduced to outsourcing-related risks), they provide a more holistic view on the outsourcing process.

Information security risks not only appear in a particular phase of the outsourcing process. The mitigation of security risks must be seen as an on-going task. Risk management must not stop after outsourcing IT services. Outsourcers need to retain highly skilled security and risk management professionals in order to continuously manage the outsourcing relationship and thereby reduce potential risks.

2.4.3 Marshall et al. – The Dynamic Outsourcing Process

After reviewing different approaches promoted by practitioners, we should also have a look at an outsourcing framework developed by researchers. In 2005, Donna Marshall, Richard Lamming, Brian Fynes and Sean de Búrca published

---

[79] See BSI (2005, p. 14)
[80] See BSI (2005, p. 77 ff)
[81] See BITS (2003)

a paper in the *International Journal of Logistics*: *The Development of an Outsourcing Process Model*.[82] I decided to present their model here instead of many other outsourcing frameworks because it combines two valuable concepts that influence the outsourcing process:[83] *a dynamic four-stage outsourcing process* and *a clustered list of external factors*[84]

Environmental Level

Politics / Regulations
Technology
Society
Industry competition

Organizational Level

Strategy
History and critical incidents
Stakeholder demands
Resources

Individual or Group Level

Politics
Power
Control of resources
Incomplete information

| Idea Formation | Evaluation | Management | Outcome |

Fig. 2.3. Dynamic Outsourcing Process Model by Marshall et al.

The four stage outsourcing process Marshall and her colleagues describe consists of *Idea Formation*, *Evaluation*, *Management* and *Outcome*.[85] They base this process on Zhu, Hsu, and Lillie (2001) and Lever (1997) but also conducted field studies. Marshall et al. argue that traditional outsourcing models are not sufficient because they usually regard the outsourcing process as a linear task.[86] Each phase is started after the previous one is properly completed. In reality, this is not the case because the outsourcing process

---

[82] See Marshall, Lamming, Fynes, and de Búrca (2005)

[83] Those insights are not new to researcher and practitioners but Marshall et al. describe them in a very concise manner, combined into a single model. See figure 2.3

[84] Those external factors can be regarded as potential security risks.

[85] See figure 2.3 and Marshall et al. (2005, p. 357)

[86] See, for example, BCG's outsourcing cycle (section 2.4.1)

needs to be highly dynamic. *"[T]he outcome of one outsourcing process will affect later outsourcing processes, and findings at one stage of the process may provide an incentive to return to a previous stage for reassessment [...]"* This is not only true for the decision whether or not to outsource a particular service but for the entire outsourcing relationship with the service provider. It explains why ongoing supervision or rather close collaboration with the outsourcing provider is crucial. Companies that outsource some of their services need to retain highly skilled personnel that can manage the relationship with the service provider, regularly reevaluate the needs of the own firm, assess the quality of outsourced services and in the worst case select a new vendor and manage the migration from the old to the new one.

The second insight Marshall and her colleagues present is that there are several factors that influence the outsourcing decision and the outsourcing process. These factors can be clustered into distinct groups. Marshall and her colleagues aggregate the factors, which they call forces, on three levels: *environmental forces*, *organizational forces* and *individual and group forces*

Environmental forces include the political situation at the outsourcing destination, regulatory limitations, legal regulations, the market of outsourcing providers, available technology, etc. One level lower, on the organizational level, the outsourcing provider itself is reviewed. Its financial situation should be analyzed, references checked and its human and technical resources scrutinized – all with the goal to assure that the provider will be able to provide the demanded services at the desired quality for the entire outsourcing period, which is often indefinite. The last and lowest level is the one of the individual employee (or a group of employees) working for the outsourcing provider or the company that would like to outsource. On the client's side, the outsourcing decision might for example be politically driven. There might be personal problems between managers and people within the IT department or employees fight for positions in the firm. An outsourcing decision might be made based on the unreflected belief that everyone outsources and since it 'saves a lot of money' it must be the right decision and needs to be made.[87] There is always an information asymmetry between the employees and managers of a company. Regarding the information flow between an outsourcing client and its outsourcing provider, the information asymmetry is even larger. Personal agendas of the outsourcing provider's employees are totally hidden from the outsourcing client. It is hard to bind the provider by contract to the provision of services by particular employees. Fluctuation can be analyzed upfront as a general characteristic but the importance of individual employees and their commitment to their job and their employer is largely unknown. These factors can be regarded as potential security risks that need to be analyzed and managed.

---

[87] This belief can even be stimulated by agreements on objectives that can seemingly be reached more easily by outsourcing services (and thereby reducing costs).

By splitting the factors that influence outsourcing processes and relationships into three levels and making them an integral part of the process, Marshall and her colleagues provide an excellent high-level approach to analyze outsourcing risks. I will make use of their levels (environment, organization and individual/group) throughout this thesis. We should further keep in mind that outsourcing processes are highly dynamic and that companies should organize their own processes in an agile manner so that they can react to sudden changes.

2.4.4 Discussion of the Outsourcing Process and Potential Risks

In the previous sections, we reviewed three process models with different foci. One framework by a consultancy, one best practice framework by practitioners and a generic process model, developed by a group of researchers, were presented. In order to merge the insights from all models, we will look at potential risks and the mitigation of those on all three levels of the dynamic process model by Marshall et al.

The levels that Marshall and her colleagues define are environmental forces, organizational forces and individual/group forces. As mentioned earlier, every level exhibits potential threats that can compromise the confidentiality, integrity or availability of data and services. Those risks need to be analyzed and managed. Therefore, a screening of potential outsourcing providers should be made on all three levels. It is a very common flaw that screenings are mainly conducted on the upper two levels, the environmental and the organizational level. Strategy consultancies like BCG and McKinsey usually analyze the outsourcing destination regarding its outsourcing provider availability and the cost saving potential for their clients. An assessment of potential security risks on the environmental level (political stability, legal regulations, etc.) or even the provider screening is not part of their core competencies. An in-depth analysis of environmental risks is mostly left to more specialized consultancies or the outsourcing client itself. During this second phase of the screening process, experts screen the target market for potential outsourcing providers. Longlists of potential providers are compiled which are reduced to shortlists after a short, rather superficial assessment of the firms. The remaining providers are assessed more extensively and reduced to a very limited number of companies, often only two or three. These are scrutinized thoroughly in order to find the right partner and to reveal potential problems as early in the process as possible. The later problems are discovered, the higher the costs of fixing them. If services are already outsourced, the change to another provider is a lot more costly than investing marginally more time into the selection at the beginning of the process.

The assessment that is made for selecting the most suitable outsourcing provider and for minimizing outsourcing related risks is called *due diligence*. According to the BITS Framework,[88] due diligence should cover

---

[88] See section 2.4.2

the following areas:[89] *Corporate Structure, Business Strategy and Reputation, Financial Analysis, Assessing Audits and Assessments, Service Provider Maturity, Privacy and Confidentiality Considerations, Assess the Service Provider's diligence in legal, regulatory and compliance areas, Determine the Service Provider's technology and systems architecture, Determine the Service Provider's reliance on other third-party service providers, Determine what impact the Service Provider will have on other Service Provider relationships that already exist in your network, Determine service availability offerings and their link to requirements, Exit Strategy Considerations* and *Disaster Recovery/Business Continuity Requirements.* Reviewing this list, it becomes obvious that due diligence is a large task. As said earlier, it is highly important to seriously go through this assessment process and not save too many resources in this early phase of the outsourcing process. A multiple of the saved expenses will be required when one has to change outsourcing providers at a later stage.

One major problem of the screening process is that issues concerning own employees and the outsourcing providers employees as well as the intercultural fit between these two groups are often overlooked. The *BITS Framework,* which consists of 125 pages, mentions the word *culture* only four times and treats it as a minor aspect. The IT Baseline Protection Manual (2922 pages) does not even once mention the word culture in the context of national or regional cultures.[90] The focus on the environmental and the organizational level and the lack of screenings on the individual or group level can be explained by two reasons:

Individual and Group Factors are Hard to Measure

In contrast to environmental and especially organizational aspects, behavior of individuals and groups is hard to measure. Corporate details like the shareholder structure, the financial situation, the size of previous outsourcing deals, etc. are relatively easy to gather. Concerning the individual level, it is almost impossible to compile quantitative figures that can be used for comparing different outsourcing providers. Even with a profound knowledge of the target culture and if due diligence experts manage to compile a list of figures concerning the behavior of the outsourcing providers' employees, the anticipation of potential security risks is highly sophisticated.

Information Asymmetries can Help Providers

The analysis of the behavior of another company's employees is extremely hard to accomplish. The other firm might not want their employees to be

---

[89] See BITS (2003, p. 19 ff.)

[90] The word culture is used nine times but only in the context of organizational culture – *security culture* or *communication culture.* For the difference between national and organizational (or corporate) culture, see section 5.3.

screened. From an outsourcing provider's perspective, it is not always desirable to reduce information asymmetries. It is interested in an excellent result and can therefore give orders to its employees to behave in a specific manner for a short period of time. Analyzing future behavior and resulting security risks is even harder in offshoring relationships because of the regional distance and cultural differences. The outsourcing client's experts might not speak the same language as the outsourcing provider's IT staff and they are often not aware of cultural characteristics of their outsourcing destination.

Up to now, there is no research analyzing culture and its impact on information security. There is no framework that can be used for predicting security threats based on cultural characteristics. My goal is to work towards such a framework. By linking cultural models with security threats I found in the outsourcing sector in China, I make a first step toward the integration of intercultural issues into due diligence.

2.5 Concluding Remarks

Societies and businesses are in a transformation process. Isolated entities turned into hierarchical structures which have been breaking apart in the last decades. Decentralization of societies and businesses seems to be inevitable. Outsourcing of services and a boom of the freelancing market is the logical consequence. The same decentralization can be observed for IT systems. Information security management has to adapt to these changing conditions. In this chapter, the concepts of information security and outsourcing were defined and recent developments in both fields were sketched out. A continuation of the outsourcing trend requires a security strategy that includes partners and providers. The selection of providers but also the management of the outsourcing partnership should be done by following a well-defined process. One major problem is the information asymmetry between outsourcing providers and their clients. Especially a solid judgement of the behavior of a potential provider's employees is hard to achieve. Up to now, there is no framework for analyzing cultural characteristics and their impact on outsourcing relationship. In the course of this thesis, I will start to close this gap and shine light on the relation between culture and information security.

3

Outsourcing IT Services in China

When asked about outsourcing destinations, people often respond 'China and India'. However, the knowledge of the Chinese outsourcing market is limited. India is considered an excellent provider for software development and service outsourcing. China, on the other hand, is often judged skeptically. Managers are afraid of doing business in China, not to mention outsourcing their IT services to a Chinese provider. In this chapter, I compare the outsourcing conditions in China and India and sketch out scenarios for future development. Afterwards, we will have a more realistic picture of the outsourcing market in China, understand the prejudices of foreign managers and will learn how to predict future developments in a systematic manner.

3.1 The Maturation of China's IT Outsourcing Market

China and India are often considered to be complementary economies. China is the *world's workshop* and India provides *back office services* for companies worldwide.[1] Even though China is portrayed as the factory of the world, providing cheap and unskilled labour, it is rapidly stepping up the value chain.[2]

Chinese companies start adapting international practices and display their experience in form of certifications. According to Shan Qingjiang, deputy director-general of the Department of Scientific and Technological Development and Technology Trade of the Chinese Ministry of Commerce, there were 87 software outsourcing service providers in Shanghai, as of November 2006,

---

[1] The Economist (2006)
[2] Lieberthal and Lieberthal (2004, p. 6 ff.)

that reached a CMMI[3] level of 3 and above.[4] This suggests that firms in China recognize the software outsourcing market as an interesting growth opportunity and are able to sustain a certain level of process quality. The growth of the Chinese outsourcing market is not only driven by the market but also by the government. In 2006, China's Ministry of Commerce launched the *1000-100-10 Project* as part of China's 11th Five-year Plan. The goal of the project is described as follows: *"China will select 10 cities to become internationally competitive outsourcing bases. It aims to attract 100 world-renowned multinational companies to outsource various services to China, handled by 1,000 outsourcing service enterprises."*[5] Together with the global growth of the market and improvements of the legal conditions in China,[6] this is one of the reasons why China is expected to gain a large share of the service outsourcing market in the upcoming years.

However, there are a couple of obstacles that need to be overcome. As for the IT service outsourcing market, American and European companies are still afraid of unreliable infrastructure and intellectual property right infringements if they outsource IT services to Chinese providers. Furthermore, they are worried about cultural differences that might pose threats on their outsourcing deals. Despite these reservations, outsourcing IT services within China, as opposed to outsourcing to China, is already fairly common. Many wholly foreign owned enterprises (WFOEs), joint ventures and domestic Chinese companies outsource their IT infrastructure and other IT-related services to providers in China.

The market underwent a dramatic rise in demand when China's banking market was fully opened to foreign banks in December 2006. The market leaders (Citibank, HSBC, Standard Chartered, etc.) opened hundreds of new customer centers in 2007 and were not able to provide all IT services in-house. However, especially in the banking but also in many other knowledge-intense sectors, the unknown security level of outsourcing providers is a risk which counters their outsourcing desires. As mentioned above, first Chinese outsourcing providers try to overcome those reservations by external (security) audits. But the fear is more deeply rooted in the minds of foreign managers. In many cases, it cannot be overcome by a simple signal like a certification. Many managers do not understand the business environment that China provides. Therefore, they are afraid of outsourcing to but also within China. The big question is where those judgements come from and if they are justified.

---

[3] *"CMMI (Capability Maturity Model Integration) is a process improvement maturity model for the development of products and services. It consists of best practices that address development and maintenance activities that cover the product lifecycle from conception through delivery and maintenance."* See CMMI Product Team (2006)

[4] Shan published this number at the Global IT Outsourcing Summit 2006 in Shanghai (November 18th, 2006).

[5] See Yan (2006)

[6] For more information on China's legal system, please see section 4.3

Concerning India, the market leader in the IT service and business process outsourcing field, the judgement is very different. This is a valuable advantage for Indian firms. In the following, I would like to give a brief overview of the conditions for outsourcing and the outsourcing markets in China and India. In the course of this thesis, I examine China's outsourcing market in depth, analyze if the prejudices of foreign managers are justified and scrutinize how risks can be minimized.

3.2 China versus India

China and India display extraordinary economic growth, striving to regain the leading roles in global business they held for centuries. Their growing impact on the world economy, not only as cheap production environments but also in the field of IT services, is doubtless. Due to their combined power, there is a lot of speculation on how they alter the global business world. The main focus of this thesis lies on the outsourcing sector. Despite many similarities in this field, China and India are considered two distinct outsourcing locations. As I mentioned earlier, China is seen as the factory or rather sweatshop of the world, India as the world's service center. The reasons for those different images, and if the image does reflect the real world, can only be understood by looking at China and India in depth.

In this section, I describe the conditions for outsourcing in China and India and the state of their outsourcing markets today. Furthermore, based on a scenario analysis that was conducted by James M. Popkin and Partha Iyengar,[7] I sketch out different paths for China's and India's future. I present possible scenarios for their roles in the outsourcing market in 2012. This section is meant to provide the context necessary to understand the current outsourcing debate. Furthermore, it provides insights into outsourcing conditions in China and India and the future development of their outsourcing markets.

3.2.1 Conditions

In the following, the conditions for outsourcing in China and India are compared based on four characteristics: *General Human Development*, *Education*, *Use of Communication Technology* and *Governance Indicators*. The main sources of the data are the World Development Indicators (WDI) by the World Bank and the Human Development Reports by the UN Development Program.

First, I would like to compare the development of China and India as a whole. As part of the Human Development Reports, the UN Development Program defined an indicator called *Human Development Index*. It is an aggregate

---

[7] Popkin is a group vice president, Iyangar a research vice president at the analyst firm Gartner. The scenario analysis approach they use is described in Schwartz (1996).

of various other values and determines the overall level of human development in numerous countries. China ranks 81st (HDI value = 0.777) as compared to India at rank 128 (HDI value = 0.619).[8] One important sub-indicator is the child mortality rate. In India, 76 out of 1000 children die before the age of 5. The figure in China is less than a third (24 per 1,000).[9]

Concerning the development of the outsourcing sector, especially in the field of IT services, the education system plays a crucial role. In 2007, 9.1 out of 100 Chinese aged 15 or older were considered to be illiterate. This is an extremely low figure compared to an illiteracy rate of 39 percent in India.[10] The gap between both countries is similar for youth illiteracy rates (aged 15-24) so that this situation is unlikely to change in the near future. In 2006, 75 percent of Chinese (out of the number of people in the theoretical age group) enrolled in secondary education in contrast to 54 percent in India.[11,12] In China, 22 percent of the people in the theoretical age group enrolled in tertiary education as compared to 11 percent in India.[13] All of these figures show that the education level in China is significantly higher than in India.

One aspect of the *Millennium Development Goals*, an initiative of the United Nations, is a goal called *Develop a Global Partnership for Development*.[14] This goal is broken down into several targets. One target, that is highly relevant for us, is target 8.F: *In cooperation with the private sector, make available the benefits of new technologies.* Success is measured by examining the number of users of different telecommunication technologies compared to the entire population. Concerning the use of communication devices, China is far ahead of India. In 2005, China had 302 cellular subscribers per 1,000 people plus 269 telephone mainlines. India only had 82 cellular subscribers and 45 telephone mainlines per 1,000 people.[15] Even more relevant for our topic is the percentage of Internet users in a country. In China, 8.5 percent of the population used the Internet in 2005, compared to 5.5 percent in India.[16]

---

[8] Japan = 8th/0.953, USA = 12th/0.951, Germany = 22nd/0.935; data from 2005

[9] This indicator is called *mortality rate, under 5 years (per 1,000)*. See World Bank (2007)

[10] See UNDP (2007)

[11] The real definition is slightly more difficult. For the exact definition, please refer to the *World Development Indicators*. See World Bank (2007)

[12] India's figure is from 2005 because no data was available for 2006.

[13] See World Bank (2007)

[14] See United Nations (2008)

[15] See UNDP (2007)

[16] Please note that data from other sources, reflecting recent developments and stating figures for 2007, vary greatly from these figures. Due to a rapid distribution of technology, they are two to three times as high as the figures from 2005. In 2007, some sources even see India slightly ahead of China. However, more current data is inconsistent so that I used data from 2005.

The fourth field of characteristics consists of governance indicators.[17] The Worldwide Governance Indicators (WGI) project,[18] started by the World Bank, aggregates indicators from various other organizations to rank countries based on their governance. These indicators are clustered into six dimensions of governance: *Voice and Accountability*, *Political Stability*, *Government Effectiveness*, *Regulatory Effectiveness*, *Rule of Law*, and *Control of Corruption*. All six governance dimensions represent percentile ranks. A higher percentile rank stands for better governance because it says that more countries rank lower. 90 percent, for example, means that an estimated 90 percent of countries rank worse and an estimated 10 percent of countries rank better on this dimension. Altogether, the WGI project ranks 212 countries and territories.

Figure 3.1 compares the ranks of China and India on these six governance dimensions.[19] The four dimensions with the strongest influence on outsourcing deals are political stability, regulatory quality, rule of law and control of corruption. The ranking of China and India on these dimensions is mixed but the overall level of governance is higher in India. China provides a more stable political situation, while India has a better legal situation and corruption is less of an issue. The regulatory quality in both countries is almost the same. By adding Japan, the United States and Germany for comparison,[20] we see that China and India rank fairly similar on all dimensions, except voice and accountability. The governance level of both countries is significantly lower than the level in the other three countries.[21]

Figure 3.3 shows the development of the ranks of these five countries over time.[22] For this comparison, I calculated the average of all governance dimensions. I added up all individuals dimensions for each country and divided the sum by six. This value therefore represents the overall governance level of each country.

Examining the chart, we can see that China ranks lowest, close to India. The other three countries also build a cluster. However, it is interesting to observe that the governance level in the United States seems to drop and that Japan improves its overall rating. Comparing China and India, we can observe that China's level remains fairly stable and that India manages to raise its governance level. India's improvements are primarily in the field of regulatory quality. In 2007, China received slightly lower scores than before for voice and

---

[17] For more information on governance in China, for example its legal system, corruption and political stability, see chapter 4.

[18] For a critical discussion of the project results, see Kaufmann, Kraay, and Mastruzzi (2007).

[19] The data used is from 2007.

[20] See figure 3.2

[21] See also figure 3.3

[22] Please note that the time periods are not equally long. There is no data available for 1999 and the data for 2008 is not available yet. Therefore, I had to make this minor sacrifice and display data for 1999, 2003 and 2007.

Fig. 3.1. Governance Indicators for China and India

Fig. 3.2. Governance Indicators for Various Countries

Fig. 3.3. Development of the Governance Level over Time

accountability, political stability and control of corruption. Its legal system, the regulatory quality and its government effectiveness have improved.

Highly skilled labour is an extremely important condition for providing outsourcing services. The figures on general education already gave a first insight. However, most interesting is data on education in the field of engineering, because we focus on IT service outsourcing. Research by Wadhwa and Gereffi from Duke University shows that the number of *Bachelor's and Subbaccalaureate Engineering, Computer Science and Information Technology Degrees* awarded in China totaled 644,106 in 2004, compared to 215,000 in India and 222,335 in the United States.[23] This suggests that China offers a significantly larger pool of skilled engineers. However, their research also shows that the way of calculating these numbers varies greatly amongst the three countries. The Chinese government seems to include a lot more degrees than the other two countries. Furthermore, the number of graduates does not say anything about the quality of their education. Even following the same curriculum might not produce the same kind of engineers. For adding value to the economy of their home country, they might need different skill sets. The ability to innovate does not only depend on the tertiary education system but also on the education that was received earlier and on other environmental factors like the regional or national culture. As a general remark, China's elite universities educate highly skilled engineers. However, the level of the mass tertiary education needs to be scrutinized further. Concerning the governance in China and India, both score fairly low. The governance conditions in India

---

[23] See Wadhwa and Gereffi (2005)

are slightly better than in China. At first view, the judgement of many managers favoring India over China is therefore valid. However, the difference is less striking as it was to be expected. The main indicator that lowers China's governance level is *voice and accountability*. This indicator has only a small impact on outsourcing deals. If China could improve on this dimension, or if this dimension was excluded from the study, China and India would score almost the same. It is therefore surprising that India is always regarded as the preferable outsourcing location.[24]

3.2.2 Future Development of the Outsourcing Sector

In 2007, the service sector generated 40.1 percent of the Chinese GDP. The industry sector reached 48.6 percent, agriculture 11.3. This is an increase of the share of the service sector of 7.6 percent, based on figures from year 2005 (services: 32.5, industry: 53.1, agriculture: 14.4). These numbers are contradictory to conventional wisdom. While China is known as the world's factory, producing goods for many leading industry firms worldwide, its service sector has been growing at a faster pace than its industry sector. This happened beyond the coverage of mass media and is therefore unknown to many people. In comparison, the Indian composition was 52.8 percent services, 29.4 percent industry and 17.7 percent agriculture in 2007. An increase of mere 1.4 percent of the share of the service sector (2005: services: 51.4, industry: 28.1, agriculture: 20.6).[25] The major difference between India and China is that many services in India are provided for foreign clients. China's software and IT service companies rather cater the domestic market. Almost no Chinese IT service company is known on the global stage. Software development and service companies like Neusoft, Bleum, Beyondsoft, Dalian Hi-Think Computer Technology, Chinasoft International, Symbio, Longtop, etc. are still fairly unknown. Even Chinese technology vendors[26] like Huawei, Haier, Founder Technology and TCL, giants in their industries, are hardly known outside of China. The only Chinese IT company that gained international recognition is Lenovo. It became well-known after purchasing IBM's Personal Computing Division. The situation is different in India. Indian outsourcing vendors like Tata Consultancy Services (TCS), Infosys Technologies

---

[24] Language certainly plays a role. As a former British colony, India has an advantage because English is widely spoken in business and administration. However, with more and more Chinese being able to communicate in English and the English language gaining importance in business in China, this issue is likely to loose importance.

[25] I am aware that those figures do not sum up to 100 percent. They are estimates published in the the CIA World Factbook. I assume the difference is due to rounding. Since they only represent estimates anyway, the overall development is more important than the reliability of decimal places.

[26] Those companies focus on the production of networking equipment, computers, consumer electronics, etc. instead of IT services.

and Wipro Technologies are well-known in the Western business world. They are covered by the media because of their extreme success, competing on the global market. Gartner even predicts that in 2011 these three providers will *"augment or, in some cases, replace today's acknowledged megavendors by revenue - IBM Global Services, Accenture and EDS".*[27] This underlines the fact that those originally Indian firms have become global players. They have become so international that Cyrill Eltschinger, CEO of Softtek China and founder of I.T. UNITED,[28] asks the question of how Indian they are after all. All major Indian IT service providers have established subsidiaries in China. They started building a workforce of highly skilled Chinese employees and 'outsource' projects to their Chinese branches.[29] This is an excellent sign of improvement of the Chinese environment and speaks volumes about the quality of the Chinese work force.[30] Chinese firms need to open up to the global market in order to receive recognition and to gain presence in international media. Today, they are still *"years behind India's [IT services firms] in stature and scale".*[31] However, with improving conditions and a consolidation of the Chinese IT outsourcing market, Chinese vendors are likely to become global players in the upcoming years. Improvements of the Chinese outsourcing environment are also acknowledged by international analyst firms. IDC, for example, even predicts *"Chinese Cities to Overtake Bangalore, Manila and Mumbai as Highest Ranked Global Offshore Delivery Centers by 2011".*[32]

By means of scenario analysis, James M. Popkin and Partha Iyengar sketch out three possible scenario paths for China's IT landscape in 2012. They call these scenarios: *Isolation/Protectionism*, *Entrepreneurial* and *China Inc.*[33] Isolation/Protectionism means that the Chinese government reverses its liberalization efforts. Domestic standards and strong government regulation would isolate China. The entrepreneurial scenario describes China as a global player, further opening its markets to foreign companies. In this scenario, the role of the government would diminish, productivity and living standards would improve. China would promote and adapt international standards as opposed to domestic ones. It would stabilize and enlarge its role as a technology innovator. This innovation would mainly be achieved by the private sector. The market would govern domestic and international business activities. In the last scenario, China Inc., the Chinese government would continue its current path. It would slowly retreat from the economic playing field. It would en-

---

[27] See Iyengar (2008) or `http://www.gartner.com/it/page.jsp?id=741012`

[28] I.T. UNITED, a leading Chinese IT service provider, was acquired by Softtek in 2007.

[29] See, for example, Eltschinger (2007, p. 51 ff.)

[30] Of course, some offices were also opened because their clients demanded a local presence and to cater the local Chinese market. However, the Indian firms also serve projects for clients outside of China from their Chinese subsidiaries.

[31] See Popkin and Iyengar (2007, p. 34)

[32] See `http://www.idc.com/getdoc.jsp?containerId=prSG20768607`

[33] See Popkin and Iyengar (2007, p. 50 ff.)

courage the private sector to innovate but navigate the country through the innovation process. This path is similar to the entrepreneurial one. The major difference is that China Inc. implies a continuation of strong government involvement (even though diminishing). Hierarchical structures persist. The entrepreneurial path shows a decentralization of business activities. The private sector blooms without government intervention. Private companies innovate and thereby become global players. The China Inc. scenario is the most likely development in the upcoming years. Popkin and Iyengar rate *"the likelihood of this outcome a 70 on a scale of 100. [They] rate the entrepreneurial path a 20 and the isolation/protectionism path just 10 on a scale of 100."*[34] They also define a fourth scenario, China becoming the *World's (Non-IT) Factory*. However, this scenario is so unlikely, considering China's current development, that it can be neglected. All four scenarios are presented in a matrix in figure 3.4.[35]

China as technology innovator

Entrepreneurial	**China Inc.**
20 %	70 %

Government involvement in economy

World's (Non-IT) Factory	**Isolation / Protectionism**
0 %	10 %

Fig. 3.4. China's ICT landscape in 2012, based on Popkin and Iyengar (2007, p. 51)

Besides sketching out these four (or rather three) possible paths for China's future, Popkin and Iyengar also define five milestones that can be used for monitoring the development of the Chinese IT service sector: *Beijing 2008*

---

[34] See Popkin and Iyengar (2007, p. 61)

[35] The four scenarios (and their likelihood) that Popkin and Iyengar map out for India are: *Isolated ICT Islands (20 %)*, *ICT Superpower (30 %)*, *Digital Chasm (50 %)*, and *Brain Drain (unlikely)*. See Popkin and Iyengar (2007, p. 112 ff.)

Summer Olympic Games, *Patent Performance in Information and Communications Technology*, *A National Trade Association to Promote China's ICT Industry*, *Government Ownership of Private Sector Assets* and *Promotion of China-Specific Standards*. I refrain from analyzing these milestones in depth in this thesis. On a superficial level, the following observations can be made. The Olympic Games were hosted in Beijing without any major conflicts. However, there were minor protests that were oppressed and human rights issues were covered by the international media. China's role as an innovator can be witnessed by a steep increase in patents filed by Chines firms and research institutions. In 2005, China's share in ICT-related patents was already 4.2 percent, only trailing Germany (7.7 %) and Korea (4.6 %).[36] India only ranked 18th, with a share of 0.4 percent. Furthermore, concerning the share of ICT in a country's patents relative to the share of ICT in total patents, China again ranked third compared to India ranking 29th.[37] To my knowledge, there is no national trade association in China, promoting the IT service sector, that is comparable to India's *NASSCOM*. The *China Software Industry Association (CSIA)* is focused on the Chinese software industry. It only published a short English introduction on its website instead of providing information on the Chinese software development and outsourcing sector. China still lacks a globally recognized advocate like NASSCOM, covering the software but also the service industry.[38] Concerning the government ownership, as in recent years, China continues to privatize state-owned enterprises. Also government intervention in the market is decreasing. Instead of introducing China-specific standards, China has been contributing to the development of international standards.[39] By reviewing the five milestones, the following assessment seems most appropriate: In the past year, since the publication of Popkin and Iyengar's work, China has continued to follow the most likely path, China Inc., rather striving for the entrepreneurial scenario than isolating itself. China's

---

[36] See OECD (2008, p. 15)

[37] China only trailed Finland and Singapore, both traditionally extremely focused on the ICT sector. See OECD (2008, p. 14)

[38] Zhonghua Qu and Michael Brocklehurst wrote in a 2003 paper in the *Journal of Information Technology*: *"It is [...] very difficult to find trustworthy information about Chinese suppliers, particularly in English, through the Internet or other media. India has set up an efficient organization, the National Association of Software and Services Companies (NASSCOM), which provides abundant quantities of reliable information, including individual supplier profiles, through the Internet. It also builds up a network among Indian suppliers. In contrast, the China Software Industry Association, as a government-managed organization, provides little helpful information for offshore customers. This inevitably pushes up the transaction costs for companies considering outsourcing to China."* See Qu and Brocklehurst (2003, p. 64)

[39] In the past, the Chinese government has tried to force own standards (e.g. WAPI, a Chinese national standard for wireless networking, see section 4.4.1). However, China has changed its course and increasingly contributes to international standards.

environment can be expected to improve in upcoming years which will help Chinese companies to successfully compete on the global market.

3.3 Common Reservations about China as an Outsourcing Destination

Based on the figures above, describing China's readiness as an outsourcing location, China seems to be on the right track to become one of the key players in the IT services outsourcing market in the near future. It is therefore threatening India by changing its role from the world's factory into a service outsourcing destination with highly skilled labor. Despite rapidly improving conditions, not only but also on the legal side, many companies still worry about outsourcing within or even to China. Their reservations are normally not based on empirical data or own experiences but rather a feeling that has established as common reasoning.

John C. McCarthy, Vice President and Principal Analyst at Forrester, summarizes the public opinion by referring to a recent study Forrester conducted in the outsourcing sector:

> The consensus among interviewees was that China still has not overcome clients' concerns about limited English skills, attrition, and weak intellectual property protection.[40]

Even though this is only a superficial explanation for foreign managers' reservations, it provides some insights into potential problems.[41] In the outsourcing debate, outsourcing risks are equated with general business risks that companies face in China. Some of these general challenges are described by London-based law firm KSB Law as *Macro economic*, *Regulatory*, *Risks associated with choosing your partner*, *Management of the supply chain*, *Communications (language and culture)*.[42,43] Even though this list is not empirically substantiated, it provides another view on the general perception of business risks in China.

Whichever source is examined, the general perception is that *outsourcing to China is risky*. Since this and similar phrases are continuously repeated in the media, they not only reflect but also form the public opinion. Massive opportunities that China as a market and as a services provider offers are countervailed by the feeling that *doing business in China is risky*.

---

[40] See McCarthy, Ross, Bartolomey, and Thresher (2007)

[41] For more information on China's role as an offshore location, see also McCarthy and Hudson (2005).

[42] See Facey (2008)

[43] Kennedy and Clark provide further information on legal risks threatening outsourcing to China. See Kennedy and Clark (2006)

3.4 Concluding Remarks

Today, China is already a major player in the IT services field. It is likely to gain a larger market share in the future. Many conditions in China are comparable to India. While India has the language advantage and a slightly better regulatory environment, China's education system is better suited for educating its population and the use of telecommunication technology is widespread. Furthermore, the environment that China provides is improving rapidly. If this process continues, China can challenge India's leadership role in the IT outsourcing sector in the future. However, for now, India's dominance is still uncontested. One major reason is the different conception of the business environments in China and India. Many companies do not see the improved conditions in China and the press coverage on China is still rather negative. Very often, companies and individuals cannot name specific problems. However, in the public opinion, China is a difficult place for doing business. This preconception is understandable considering that many foreign companies burnt their finger and a lot of money entering the Chinese market. However, there is very little literature on the Chinese outsourcing market. The few studies that exist note that China's legal and cultural environment as well as its infrastructure disqualify it as an outsourcing location. Those statements are rather broad. In many cases this fear is not empirically grounded in data but just summarizes the public opinion. In order to understand how much of this negative preconception is actually valid, we need to conduct research ourselves. Literature research can provide a first impression. However, since studies in this fields are rather scarce and superficial, I had to collect empirical data myself. I went to China and immersed into the outsourcing and information security industry in order to deepen my understanding of the situation. The results of my study are presented in the course of this thesis.

Part II

The Chinese Outsourcing Environment

Conclusion

The Chinese Outsourcing Environment

Cultural Security Issues in China

Foundations

environment

organization

individual / group

personality

culture

human nature

4

Some Findings – China's Outsourcing Environment

A stable business environment is an important precondition for successful outsourcing deals. Many foreign managers are afraid of the Chinese outsourcing environment and believe that its deficiencies lead to security threats. This chapter is dedicated to the presentation of some of my research findings. It describes some of the security threats that companies face while outsourcing IT services in and to China.[1] These insights are based on the interviews I conducted in China and on a comprehensive literature review. The reason for my strong emphasis on the word *some* is that I would like to underline that my most significant findings are not presented in this chapter but in chapter 6. The next section, which can be seen as an introduction to this chapter, explains the separation of my research results.

4.1 Interview Results – Outsourcing in China

By conducting problem-centered interviews in China, I gained a broad understanding of information security risks that companies face while outsourcing IT services in or to the People's Republic of China. While conducting those interviews and reviewing the first results, I realized that I was collecting a large variety of seemingly unrelated security threats. I use the word *seemingly* here because I believe that culture always sets a context for other regulators and frames potential risks. Therefore, most security risks are related to one another by the concept of culture. However, this link is not always obvious and when I talk about culture-based security threats in this thesis, I focus on risks related to human behavior instead of regulatory aspects.

The large list of security threats I found had to be structured in a adequate manner for presenting them in this thesis. When I thought about how

---

[1] A comparison of environmental preconditions (governance, education, etc.) in different countries is presented in section 3.2.1. This chapter focuses on the Chinese outsourcing environment and environment-related security threats.

to cluster them, I first intended to use the four regulators by Stanford law professor Lawrence Lessig – *Law*, *Norms*,[2] *Architecture*[3] and the *Market*. Lessig became well-known for his theory that the Internet (or the cyberspace) is not unregulable, as many researchers and practitioners postulated before, but that its code is a regulator on its own. Code has the same power as the other regulators. To say it in Lessig's words *"Code is Law"*.[4] Lessig argues that the four regulators, *law*, *norms*, *architecture* and the *market*, regulate our entire world. Many researchers see Lessig's regulators as related to cyberspace. However, this is only one application of them. Lessig himself introduced his regulators in his essay *The New Chicago School* in a much broader context. He says that *"[b]ehavior is regulated by four types of constraint"*.[5] He writes about regulation in general and not regulation of cyberspace in particular. His four-regulator framework would have provided me with a generic cluster that I could have used for structuring my thesis. However, when I started sorting my research results, I realized that some security issues did not quite fit into his framework. Even more importantly, using his framework, I would have mixed all aspects that are related to one regulator regardless of on which level they influence society. I would have mixed issues on the level of continents with those on the level of countries, companies and even on the level of individual employees. I believe a hierarchical analysis of regulators and security threats is more insightful and more practical because it can be integrated into the outsourcing process more easily. During the decision making process and due diligence, one normally follows the hierarchy downwards, analyzing outsourcing destinations (China, India, etc.) before assessing particular providers within those countries. I needed a framework that supports this hierarchical order.

In sections 2.4.3 and 2.4.4, I introduced the dynamic outsourcing process model developed by Marshall et al. Besides the four-step dynamic outsourcing process it also includes a three-level model of factors that influence the outsourcing process. Those three levels are *environmental factors*, *organizational factors* and *individual/group factors*.[6] By regarding those levels as risk levels, I could perfectly assign my research findings to those three levels. I present my insights by going through this structure.

On the uppermost level, the environmental level, all security aspects concerning the outsourcing destination China as a whole are subsumed. Legal and political aspects, infrastructure issues, etc., belong to this level. These are all aspects that individual providers cannot influence. During the interviews, I found many regulatory issues on this level that have an impact on information

---

[2] Norms can be understood as social or cultural norms. A profound definition and explanation of norms can be found in section 5.4, especially 5.4.1.

[3] Architecture is also sometimes interpreted as infrastructure or code.

[4] See Lessig (1999, p. 3) or Lessig (2006, p. 1)

[5] See Lessig (1998b, p. 662). Lessig already mentioned the regulators in Lessig (1998a).

[6] See sections 2.4.3 and 2.4.4 as well as figures 1.4 and 4.1

Environmental Level

Politics / Regulations
Technology
Society
Industry competition

Organizational Level

Strategy
History and critical incidents
Stakeholder demands
Resources

Individual or Group Level

Politics
Power
Control of resources
Incomplete information

Fig. 4.1. Risk Levels as in Marshall et al. (2005, p. 357)

security in outsourcing relationships in China. The second level, the organizational level, covers all aspects that are related to particular organizations, individual outsourcing providers in our case. Since I did not attempt to compile a survey covering particular service providers but would like to provide generic insights, I made an important decision. I excluded this level from my analysis. If security issues affect the outsourcing relationship on an organizational level but the problems are rooted in the individual/group level, which of course very often happens, I assigned those aspects to the individual level. This particular chapter is devoted to my findings on the environmental level. As I said, I excluded the organizational level and the reasons for not presenting the individual level in this chapter are pointed out at the end of this chapter.[7]

This list of security threats and environmental factors that affect information security is not a complete checklist that covers all potential risks. It is not meant to be exhaustive. Its purpose is to provide insights into security problems that outsourcing clients face when outsourcing in or to China. Many of those aspects are seldom discussed in outsourcing guidelines but should still play a prominent role when considering whether or not to outsource and which destination to select.

---

[7] See section 4.6

4.2 Country Risk

Under the label of *country risk*, I subsume many aspects of stability. I do not focus on single outsourcing providers and their stability (in financial terms, for example) but examine the stability of a country as a whole. If the environment at an outsourcing destination is unstable – we will soon see what I mean with instability – the availability of outsourced services cannot be guaranteed. Of course, besides stability, there are many other security risks related to the outsourcing destination like language barriers, geographic distance, infrastructure issues, availability of knowledge workers, legal regulations, etc. However, this section addresses the stability issue. But also the stability issue is not discussed in its entirety. This thesis cannot provide an all-embracing description of the instability risk in China because for each of the risks we will touch, many Ph.D. theses can be written. Some other country-related aspects like infrastructure issues and legal regulations are discussed in later sections.[8] Others like language barriers and geographic distance are only mentioned, but not analyzed in depth, due to their obviousness. They are touched in the chapters devoted to culture-based security risks.[9]

When outsourcing to China, there are various future developments that can lead to instability. Companies outsourcing in China worry about a couple of scenarios that would seriously affect their outsourcing activities. Those risks can be clustered and presented on three distinct levels – *Economic Stability*, *Social Stability* and *Political Stability*. Those areas are certainly interlinked and influence one another. Risks can hardly be assigned to only one level. However, I try to stick to these clusters and will give a brief introduction into concerns regarding each of those levels.

4.2.1 Economic Stability

> It does not matter if a cat is black or white, so long as it catches mice.
> Deng Xiaoping, 1962[10,11]

This quote, which stands for Deng Xiaoping's open-door and reform policy, depicts the pragmatic attitude of most Chinese towards their economy. It does

---

[8] For infrastructure issues, see section 4.4. Legal regulations are presented in section 4.3.

[9] Chapter 5 highlights the influence of human behavior for information security and introduces cultural models. Chapter 6 links cultural models with culture-based security threats I found in China.

[10] See Shambaugh (1995, p. 88). In the original saying, coming from Deng Xiaoping's native province Sichuan, the word *yellow* is used instead of *white*. See Stewart (2001, p. 64) and He (2001, p. 24)

[11] There is a variation of Deng's quote that has been used by many Chinese for expressing their anger with the corrupt system: *"No matter whether it is white or black, it is a good mouse if it can escape from the cat."* See He (2001, p. 25)

not matter how the system works and how it is called as long as it blooms and fulfills a righteous purpose. However, in the years after his statement, Deng was attacked for his 'reactionary propaganda'. Today, there is not much left of Mao's thinking and China has greatly opened up to world economy. And China has managed to steer through the problems of global economy in a striking manner. China and India successfully managed to survive the Asian Financial Crisis which affected the lives of millions of Asians in the late 1990s. Their economies are soaring and have experienced a steady and highly impressive growth. China even has become the largest recipient of foreign direct investment.[12]

Despite those achievements and China's stability during the Asian Financial Crisis, voices are getting louder that warn against an economic backlash or even a breakdown in the near future. Deloitte Research conducted a survey in which they identified seven risks of doing business in China:[13] *Financial System*, *Currency revaluation*, *Economy overheats*, *Economy falters*, *Problems of state owned enterprises and the transition to privatization*, *Trade conflict*, and *Income disparities*.

The fragility of its financial system is probably China's biggest economic risk. The Chinese banking sector is dominated by four state-owned banks, *Industrial and Commercial Bank of China (ICBC)*, *Bank of China (BOC)*, *China Construction Bank (CCB)*, and the *Agricultural Bank of China (ABOC)*. Those banks also account for the biggest share of loans. *"By the mid-1990s, over one-half of SOEs were making losses and about three-quarters of the loans on the books of these banks were to SOEs."*[14] Most of these loans were therefore *bad loans* – loans that are not paid back to the lender and thereby non-performing. In the late 1990s, the Chinese government took various steps to solve this issue. Amongst others, it recapitalized the state-owned banks and established four asset management companies that bought a large share of the non-performing loans from the banks.[15] According to current legislation, the banks are now required to establish a risk management and to lend money on the basis of creditworthiness (solvency). However, the government can order the banks to lend also to unprofitable businesses if it is important for the growth of the Chinese economy. This exception erodes the otherwise sound system and brings non-performing loans into the banks' portfolios. The second problem is that the Chinese government has enormously supported the U.S. dollar and deliberately kept down the value of the Chinese Renminbi

---

[12] See Stiglitz (2000)

[13] See Kalish (2004). The author of the survey, Ira Kalish, does not present his research methodology and the risks he identified are described on a highly superficial level. However, for sensitizing the reader for economic risks in the People's Republic of China, his study provides an excellent starting point.

[14] See Bonin and Huang (2001)

[15] See Ma and Fung (2002)

(RMB) in order to boost its exports.[16] As a result of the Chinese strategy, trade conflicts with other countries, especially with the United States, have emerged in recent years and quotas for goods manufactured in China have been established.[17] The strategy of the Chinese government to keep the value of the RMB down has also been taken into account by banks for granting loans and by foreign investors which further supported the manufacturing sector. If the Chinese RMB was seriously revalued in the near future, Chinese export prices would rise dramatically. As a positive effect, this would lower inflation and reduce the risk of an overheating Chinese economy.[18] The Chinese administration is slowly starting to use market-based instruments like raising interest rates for slowing down the economy and has begun appreciating the RMB against the dollar. However, it maneuvered itself into a difficult situation because economic growth is important for maintaining social and political stability.[19] Another risk source that might lead to social instability is the necessary privatization of Chinese state-owned enterprises (SOE). Many SOEs are unprofitable and can only survive (and still invest) with the support of state-owned banks. A privatization is the only logical step and would lead to higher productivity in the long run. However, a privatization would also entail a layoff of many Chinese workers. That economic growth and job security are no guarantee for the government to receive support from the public could be witnessed in India in 2004. The opposition won an unexpected victory and displaced the seemingly successful government. One major reason were growing income disparities between urban and rural population. The same situation can be observed in China. Furthermore, people living in rural areas are becoming more aware of theses disparities due to the spread of modern communication technology. This problem is discussed in detail in the next section.[20]

I started this excursus on economic stability in China with a famous quote by Deng Xiaoping: *"It does not matter if a cat is black or white, so long as it catches mice."* I also would like to end this paragraph with his quote and another one that refers to it. In November 2006, Thomas L. Friedman, au-

---

[16] Gene Hsin Chang and Qin Shao argue that the Chinese RMB was undervalued by 22.5 percent in 2003. See Chang and Shao (2004)

[17] Occasionally, incidents concerning toxic goods prompted the European Union to temporarily stop particular imports from China.

[18] The current economic growth and inflation also demand sharp increases of salaries. This might turn China into a less interesting supplier and manufacturing might partially shift to new locations like Vietnam.

[19] See my following remarks on social and political stability.

[20] The review of China's economy and its current problems is based on the study *China at a Crossroads – Seven Risks of Doing Business* by Deloitte Research (Kalish, 2004) and insights I gained while living and conducting research in China. Furthermore, all insights are triangulated by reviewing research articles and media coverage.

thor of *The Lexus and the Olive Tree* and *The World is Flat*,[21] quoted Dan Rosen in his New York Times column with the words: *"Now the cat better be green, otherwise it is going to die before it catches the mouse."*[22] This quote refers to one of the major side effect that have such a tremendous influence on the world and China in particular that they cannot be disregarded. China's rapid economic growth has been achieved by exploiting the environment. Pollution is omnipresent in China and affects the daily life of millions of Chinese. Furthermore, its staggering growth is leading the world into an energy crisis. One strategy of the Chinese government to tackle this problem was to build the *Three Gorges Dam*, the world's largest hydro-electric power plant. This project forces millions to relocate. Pollution and forced relocation, both outcomes of China's enormous economic growth, are starting to spur conflicts between government and citizens.

4.2.2 Social Stability

Even though most Chinese perceive an economic and social progress and have more money to spend from year to year, the gap between rich and poor in China is growing continuously.

Since many Chinese, especially in rural areas, believe they cannot survive with the little income they can gain in their region and certainly cannot provide their children with an opportunity to live prosperous lives, many households decide that one family member should move to the coast and become a migrant worker. Thereby they manage to realize an increase in household income[23] but accept that their children see their father or their mother only a few weeks a year. If those work as migrant workers, they often only return home for a few weeks around Spring Festival (Chinese New Year).

Chen and Fleisher wrote in 1996 that *"[a]ltering the future distribution of labor-force growth across regions is perhaps the most difficult economic and social problem facing China today"*.[24] A decade later, the question of labor-force distribution and labor mobility is still one of China's core problems. David Whitehouse states that by 2004, the number of people working in cities but registered as "agricultural" exceeded 100 million and that this figure was growing continuously.[25] Today, some coastal regions still address this problem

---

[21] See Friedman (2000) and Friedman (2005)

[22] See Friedman (2006)

[23] See Zhao (1999)

[24] See Chen and Fleisher (1996, p. 157)

[25] See Whitehouse (2006) based on Zhang (2004). Zhang (2004) quotes statistics from the Ministry of Agriculture that indicate that the number of farmers working in cities is growing by 8.5 percent annually. Since 100 million is the official number, the number is likely to be higher in reality. Other sources state numbers of 200 million and even higher.

by making use of the *hukou system*.[26,27] If the government would change their strategy and migrant workers, their families and any other Chinese from rural areas were allowed to settle anywhere they like, the population in coastal areas would dramatically increase which would create new sources of social unrest and overstrain the existing infrastructure.

But the problem of Chinese migrant workers is only one example of many. Especially in rural areas, social stability is threatened by various problems.[28] Overtaxation by local leaders and corruption are omnipresent in rural China. On the *Corruption Perception Index 2007*, which describes the degree of corruption in various countries,[29] China scores 3.5 on a 0-10 scale (0 = highly corrupt, 10 = highly clean).[30] Minxin Pei, director of the China Program at the Carnegie Endowment for International Peace, states that corruption in China is concentrated on sectors with strong state involvement. It is especially high in industries that are still subject to governmental regulation, infrastructure projects, real estate, etc.[31] As a typical example of corruption in local areas, he mentions the use of *"illegal (and sometimes violent) means to acquire farmland at low prices and later sell the user rights of the land to developers in exchange for bribes"*.[32] Two major problems are China's still underdeveloped legal system and the lax enforcement of penalties by the Communist Party.[33]

Corruption and many other problems in rural areas (including pollution and forced relocation) lead to the manifestation of a fear of the future in the minds of many peasants. They feel threatened by the government, especially by local officials, and are sometimes even afraid of loosing their homes. As a consequence, a dramatic rise in demonstrations and riots seems inevitable. As I said before, as long as there is a perceived economic progress for most Chinese citizens, countrywide uprises that seriously endanger the current system are unlikely. However, there are many regional conflicts. Zhou Yongkang, Minister

---

[26] A hukou is a residence permit that allows to live and work in a specific region.

[27] For problems with the hukou system, see amongst others Au, Nan, and Zhang (2007).

[28] As mentioned earlier, pollution is a another major problem for many peasants.

[29] To be precise, it describes the perception of the degree of corruption stated by business people and country analysts.

[30] See Transparency International (2008a, p. 27) and Transparency International (2008b, p. 299)

[31] See Pei (2007, p. 2)

[32] See Pei (2007, p. 3). In this article, *Corruption Threatens China's Future*, Minxin Pei vividly describes how corruption endangers China's economic and political future as well as its social stability.

[33] See section 4.3

of Public Security,[34] reported an increase from 10,000 mass incidents in 1994 to 74,000 in 2004.[35]

Growing inequalities, corruption, prestigious project like the *Three Gorges Dam* which demands the relocation of millions of people, dramatical pollution of the environment, etc. disrupt social stability and are likely to stir up many more riots in the future.

4.2.3 Political Stability

Concerning political stability, there are two major risks for the People's Republic of China: *rebellion against the political system* and *conflicts with regions striving for autonomy or even independence.*

The first risk means that social instability and social upheavals might lead to a rebellion against the current political system. As described before, there are various issues threatening social and thereby political stability. In recent years, the Communist Party of China (CPC) has changed its course. It tries to circumvent social unrest by economic progress. Starting with Deng Xiaoping, it has opened up to capitalist ideals. Since the 16th National Congress, private businessmen are allowed, and even encouraged, to join the party. Conservative party members and citizens oppose this new course. Another sign for the change in the Communist Party is that, already in the 1980s, it started experimenting with elections on a local level, for village committees.[36] This possibility for Chinese villagers to participate in the direction of the future course of their village, is likely to lead to more active political participation.[37,38] Besides this local participation, general elections have occasionally been on the agenda of the political elite. However, they have been deferred indefinitely because *"the time was not ripe"*.[39] These deliberate steps towards a modernization of the political system might not be enough to ensure social stability. On the other hand, they might initiate a change process that cannot be controlled by the party anymore.

The second risk that could compromise the current political system are serious conflicts with regions that strive for a higher level of autonomy. The

---

[34] Since he is an official of the People's Republic of China, again, the unofficial number is likely to be higher.

[35] See Congressional-Executive Commision on China (2005). For further information on the rise of protests in China, see also Tanner (2004).

[36] See, for example, Womack (1982); Jacobs (1991); Shi (1999); O'Brien and Li (2000) and O'Brien (2001)

[37] See, for example, Li (2003)

[38] It is important to bear in mind that besides the government committees, there is always a party committee at all levels that often influences the political course. Furthermore, the election of village committees needs to be improved so that it becomes more democratic. O'Brien recently made a proposal how to improve local elections in China. See O'Brien (2008)

[39] See O'Brien (2001, p. 411)

tibet conflict, which was recently widely covered in the news, is one example of those disputes. There are other regions like Xinjiang (Xinjiang Uyghur Autonomous Region) and Taiwan, which is administered by the Republic of China (ROC) but claimed by the People's Republic of China (PRC), that have ongoing disputes with the PRC government about their independence.

Today, news coverage of serious conflicts is censored in China but this censorship is getting harder to maintain. The Chinese blogosphere[40] is growing rapidly. This decentralized form of publishing is hard to control and news that spread over the network are almost impossible to filter.

As we saw, economic, social and political stability are highly interlinked. Only if stability can be maintained on all three levels China's outsourcing market will continue to flourish.[41]

4.3 Legal Considerations

> In theory there is no difference between theory and practice. In practice there is.[42]

Every time I think about this statement, I am reminded of the Chinese legal system. In theory, China's legal system follows a principle called *rule of law*. In practice, if we look behind the scenes, centuries of *rule by law*[43] cannot be wiped away.[44] To understand the difference between theory and practice and to discover the reasons for this gap, we have to look into the past. We need to be aware of China's history. Chinese culture has been shaped over centuries, even millennia, and affects thinking and policies today.

---

[40] The word blogosphere stands for the collection of all weblogs (also called blogs) and their interconnections.

[41] Of course, there are also other country risks like natural disasters (earthquakes, floods, etc.). There are also many other problems on an economic, social and political level. Amnesty International lists many of the risks we discussed but also addresses other problems concerning human rights in China. See, for example, Amnesty International (2008). However, those were not the ones my interviewees were worried about. They were concerned about the risks I described above – economic, social and political stability.

[42] This quote is attributed to Yogi Berra. Lawrence Peter "Yogi" Berra is a former baseball player and manager, primarily working for the New York Yankees. He is famous for his provocative statements. His supporters even invented an own name for his way of expression – Yogiism.

[43] Rule by law is also sometimes called *rule of man*.

[44] Orts (2001) provides an introduction to the meaning of the rule of law. It further explains China's development concerning the rule of law in front of China's history and tradition. Peerenboom (2002) is an excellent reference for deepening one's understanding of China's transition from the rule by law towards the rule of law. For those who are more interested in anecdotes about the Chinese legal system, Schaub (2007) is a good read.

4.3.1 Culture and Law in Conflict

According to cultural researchers Fons Trompenaars and Charles Hampden-Turner,[45] the relation between culture and law is a follows

> Culture is the context in which things happen; out of context, even legal matters lack significance.[46]

In order to understand their view on the conflict, one needs to review theories and concepts from the field of cultural studies. The insights gained can be used as a basis for explaining legal problems currently prevalent in China.

As I will explain later,[47] there is no generally accepted definition of culture. Most definitions are based on the principle that culture is formed by the interaction of humans. Culture is the bond that unites people but also differentiates groups from one another. It is formed over long periods of time. In cultural studies, culture is often visualized as an onion, composed of distinct layers. The core of a culture, which is often invisible to outsiders, consists of norms and values. Those norms and values are expressed by practices which are more easily observable.[48,49] Looking into the field of institutional economics, social norms as part of culture's core turn out to be particularly important. Social norms, together with money, human rights and language, can be seen as fundamental institutions. Law, on the other hand, is an institution that is derived from the former ones.[50] It can only exist within the scope that is set by fundamental institutions.[51] Therefore, laws are only followed by society if they adhere to the frame that fundamental institutions create. This relation between laws and social norms is not respected in China. Ethical principles, the implicit definition of a socially accepted frame, are based on cultural norms and values. Laws are normally based on those ethical principles.[52] This is not always the case in China. Various current laws were developed for stabilizing China's economy and for supporting its future growth. The protection of the rights of individuals is regarded as less important.[53] China's accession to the

---

[45] Trompenaars and Hampden-Turner are introduced in section 5.5.6.

[46] See Trompenaars and Hampden-Turner (1997, p. 8)

[47] See section 5.4

[48] See section 5.4

[49] According to Geert Hofstede, these practices are composed of rituals, heroes and symbols. See section 5.5.5 and Hofstede and Hofstede (2005, p. 6 ff.)

[50] See Picot, Dietl, and Franck (2005, p. 9 ff.)

[51] See section 5.4.1, especially figure 5.6

[52] This statement might be misleading if one does not take into account the particular group of people for which the law is introduced. Examples can be found in which a subgroup develops social norms that maximize its own social welfare within the group but discriminate people outside of it. In that instance, laws can contradict the social norms of the subgroup in order to steer their behavior for the good of society as a whole.

[53] See Chen (1999, p. 1)

WTO led to new legal regulations. These laws are therefore based on external influences.[54] They do not take into account particular Chinese characteristics and might even disrespect Chinese cultural values. This failure to comply with the rules that are set by fundamental institutions can be seen as one of the key reasons for the reluctance of many Chinese to comply with newly enacted laws.

Furthermore, the Chinese society does not have cultural or historical roots to a legal system like those prevalent in most western countries. According to Geert Hofstede, *"[i]n countries with weak uncertainty avoidance, a feeling prevails that if laws do not work, they should be withdrawn or changed. In countries with strong uncertainty avoidance, laws can fulfill a need for security [...]"*.[55] China is considered to be a country with an extremely weak uncertainty avoidance.[56] Therefore, codified formal rules, like laws, never prevailed. Instead, due to the high importance of the community and personal relationships, problems have been solved merely by social pressure based on informal social norms.[57]

Robert Ellickson observed the dominance of social norms over codified laws at a group a farmers in Shasta country, California. He describes the results of his study in the book *Order without Law – How Neighbors Settle Disputes*. He criticizes law-centric researchers and practitioners who follow Thomas Hobbes' tradition, regarding all rules of a society as solely dependent on decisions made by the government, the Leviathan, presuming chaos would prevail without the existence of a ruling sovereign.[58] On the contrary, China seems to be the perfect example of a stable society that existed for centuries without any formal kind of regulation. Social norms, as a decentralized mean of social control, have replaced the central regulator that Hobbes regarded as inevitable.

Due to a strong sense of community, the 'right outcome' is defined by one's own network of relationships and not by rules that were determined by others. In game-theoretic terms, those strong, long-lasting relationships and the social network they form can be regarded as iterated, not single-shot,

---

[54] See, for example, Clarke (2003a)

[55] See Hofstede and Hofstede (2005, p. 190). For an explanation of *Uncertainty Avoidance*, see section 5.5.5.

[56] In contrast, uncertainty avoidance is strong in most western countries, Germany in particular.

[57] The aspects of uncertainty avoidance and collectivism both play an important role in shaping the regulators prevalent in a country. Even though Japan is a country with a strong uncertainty avoidance, the dominant regulator are not laws but norms, which are rooted in tradition. This is due to the fact that in Japan the individual is less important than the group. Not complying with the rules of the group and the resulting social punishment have a stronger impact on behavior than legal documents. See Hofstede and Hofstede (2005, p. 190)

[58] See Ellickson (1991, p. 4 and p. 138)

play.[59] According to Axelrod, this repetition leads the players into adapting a cooperative strategy.[60] Complaisances and also unjust behavior get noticed but are put into a long-term context. Social norms, which the Chinese social network (Chinese: Guanxi) is based on, can be described as a scale that can be unbalanced for a short while but needs to be balanced again over time. As long as the members of the group act according to this norm, the society is stable and individuals are content. In case this norm is not obeyed for a long period of time and the scale stays unbalanced, a tension grows that needs to be released. In Chinese social groups, this often does not happen by resolving problems on a legal basis but by vigilante justice. This vigilante justice is seldom violent. It often solely means social punishment which is sufficient for protecting social stability. Economically, these two principles – balancing mental accounts on the long run and enforcement characteristics administered by the social group itself – make sense because they minimize costs for the society[61] and therefore increase its welfare. Assuming that members of a social group would like to minimize losses in social welfare, social norms are the preferred regulator.[62] Furthermore, according to Ellickson, the conflict resolution based on social norms is more socially acceptable because it does not weaken the group and the feeling of solidarity as strong as legal conflict resolution.[63]

Social regulation and the Chinese resistance to codified laws are strengthened because formal regulations and their enforcement object an important Taoist tenet which is called *Wu Wei*. Wu Wei means that one shall not act and govern every situation, especially not in an inconsiderate or even forceful manner. One should leave problems to themselves and the world (environment or nature) will lead the issue into the appropriate direction. Furthermore, many Chinese believe that serving justice by law does not work anyway. There is an old saying which literally means *the heaven is high the emperor is far away*. It can either be interpreted as *it is difficult to get justice* or as *being beyond reach of the authorities*. Over centuries, Chinese citizens made bad experiences with regulations that were decided on by individuals or small groups of people.[64] During the cultural revolution, 1966 to 1976, the legal system was completely abandoned. Lawyers and judges were sent to reeducation camps.[65] The only way to protect oneself from the arbitrariness of the red guards was through social norms.[66] Therefore, a demand for order through social norms that are rooted deep into society has developed.

---

[59] See Ellickson (1991, p. 50)

[60] See Ellickson (1991, p. 164 ff.)

[61] There are for example no transaction costs related to financial compensation and there is no need to employ lawyers and judges.

[62] See Ellickson (1991, p. 241)

[63] See Ellickson (1991, p. 243)

[64] They experienced what is known today as *rule by law* or *rule of man*.

[65] See Wang (2001, p. 12)

[66] But even those social norms could not offer full protection against Mao Zedong's followers.

Laws that were enacted due to external influences, without being based on socially accepted and appreciated values, that might even be in contradiction with the frame that was created by the fundamental institution of social norms, are disobeyed in China and often even considered as non-existent.

4.3.2 Underdeveloped Legal System

As mentioned earlier, the Chinese society has largely based its cooperation and coordination on informal rules (social norms) for centuries. However, for participating in a global economy, formal institutions are necessary. They can be communicated to people outside of the social group more easily. Robert Hall and Charles Jones argue that high productivity (high output per worker) can only be reached with regulating institutions and government policies in place.[67] Douglas North states that *"the inability of societies to develop effective, low-cost enforcement of contracts is the most important source of both historical stagnation and contemporary underdevelopment in the Third World"*.[68]

Due to these reasons, the Chinese government has decided to start the long march towards the rule of law, besides immanent conflicts between culture and law. Today, there are still many practical problems that the Chinese government has to solve. Some of those problems have emerged because of China's rapid economic progress. The legal system could not keep up with the pace the economic progress was dictating.

A large variety of laws and regulations are enacted every year. However, it is unclear which kind of regulations should be passed on which level. Therefore, local regulations are sometimes contradictory to higher level legislation. High level bodies like the National People's Congress could invalidate those lower level regulations but do not fill out this control and governance role. In theory, higher level legislation is superior to lower level legislation but courts cannot rule out conflicting lower level regulations because they are controlled by local governments.[69,70] This is the reason for many inconsistencies in legislation in different area of China. The government cannot oversee these inconsistencies and this task is even harder for individuals or corporations.

Lawyers and judges in China suffer the same problem of understanding differences in legislation. This directly leads us to another serious problem, the low level of education of the judges. Not long ago, a Chinese judge did not need any official training before coming to office. In 2002, a bar examination

---

[67] See Hall and Jones (1999). However, they further write that those laws and regulations also *"constitute the chief vehicle of diversion in an economy"*.

[68] See North (1990, p. 54)

[69] See Clarke, Murrell, and Whiting (2005, p. 43)

[70] Officially, local governments have no direct control over financial and personnel affairs at courts. But in practice, local officials directly influence important decisions. See Henderson (2007, p. 154)

was introduced that all new judges have to pass.[71] However, judges are still not required to study law.[72] The examination is the only barrier and enforcement of this rule is another issue. Donald Clarke argues that a uniform level of education would not say much since the requirements in cities and rural areas are largely different. He further questions that formal education at a research institution would necessarily better qualify judges for their role – *"to extend state power into the countryside"* – as he describes it.[73] On the contrary, he argues that filling court positions with demobilized army officers, which was very common and even today is still the case, seems more logical (even though it is the wrong decision).[74,75]

Controlling the work of judges and their courts is almost impossible. Transparency is not a design principle of China's legal system. Its operations are secret unless specific rules demand otherwise. Court documents are closed to the public and it would hardly be possible for a Chinese and impossible for a foreigner to show up and attend a hearing.[76] According to many lawyers I talked to, it is extremely difficult to get clear information on legal regulations from government offices – if so, only from informants one had previously built up personal relationships with and on their sole discretion.[77,78]

Summing up, some major problems of the Chinese judicial system are conflicts between legislation on different levels, low educated judges and government-controlled courts as well as a lack of transparency in law enforcement and legal decision making.[79] Uncertainty concerning the legal outcome in case of conflicts is a serious (security) threat for companies outsourcing their IT services within or to China. This knowledge influences their decision of whether or not they outsource to China and how to manage the outsourcing process. Many aspects I just mentioned lead us directly to another major problem of Chinese legislation and its economic, social and political system in general — corruption.

---

[71] See Yang and Ehrichs (2007, p. 54)

[72] In 1997, less than 6 percent out of 250,000 court cadres held a bachelors degree or above. See Clarke (2002, p. 19), also published as Clarke (2003b). Current figures are hard to obtain. Since the reformation of the Judges Law, judges are required to at least hold college degree. See Henderson (2007, p. 157)

[73] See Clarke (2002, p. 21)

[74] See Clarke (1996, p. 10)

[75] Private and commercial investigation agencies are often founded by the same group of people (former police and army forces) which turns out to be problematic, as we will see later in this section.

[76] See Clarke, Murrell, and Whiting (2007, p. 21)

[77] This is extremely troublesome because decisions are also based on internal regulations that are not communicated to the public.

[78] See Clarke et al. (2007, p. 21)

[79] Of course, this text can only provide a brief introduction into China's legal system. It is not meant to cover all problems but should rather give a first overview of deficiencies of the Chinese system. It builds a basis for understanding legal problems that occur while outsourcing in and to China.

4.3.3 Corruption

Clarke, Murrell and Whiting describe China's judicial system in the following pointed manner: *"[T]he legal system is a tool of governance and control and is essentially the property of government, not the citizenry."*[80] It is further used by judges and local officials for personal gain and by local businessmen for supporting or protecting their own businesses, as we will see soon.

As mentioned earlier, China scores 3.5 on the Corruption Perception Index 2007 (0 = highly corrupt, 10 = highly clean).[81] Since this score is based on the perception of business people and country analysts, it is highly relevant for our topic. Business people work in China and have made their experiences with the Chinese judicial system and country analysts provide the basis for due diligence on a environmental level (and can thereby influence the outsourcing decision). As long as Chinese courts are perceived as corrupt, this will hinder the outsourcing market to flourish. Especially if we look at the local level, the perception is consistent with reality.[82]

As described earlier, a serious problem is that courts often stick to local regulations even though higher level legislation should theoretically overrule them if they are in conflict. Thereby, local governments and business owners can assert their interests by putting pressure on local courts. Ruling in favor of local governments and businesses is common as a favor but also when judges are bribed, blackmailed or otherwise pressured. I was talking to a foreign lawyer who specialized in intellectual property infringements and has been working in this field for many years all over China. He told me that it is out of question if judges are bribable. To say it in his words: *"It [just] depends on where you are how much you have to pay."* That judges are open to bribery has many reasons. One of them is rather obvious: Chinese Judges often receive very low salaries. Many of them are paid *"substantially less than most practising lawyers and, in some provinces, even police officers [earn] more"*.[83] This explains why judges are easily seduced by bribes but also why many highly skilled graduates choose other jobs which are better paid.

With a rising importance of the judicial system, also concerning the resolution of business conflicts, corruption is becoming a bigger problem. Outsourcing clients, especially foreign ones, complain that it is hard for firms from other areas within China – and almost impossible for foreign firms – to win cases in front of courts that are based at the outsourcing providers location. As long as local officials can exercise control over their courts, these statements seem logical. There is a conflict between central and local interests, as it is often the case in China. The central government is striving to

---

[80] See Clarke et al. (2007, p. 21)
[81] See Transparency International (2008a, p. 27) and Transparency International (2008b, p. 299)
[82] The same is true for higher levels but to a lesser extent.
[83] See Yang and Ehrichs (2007, p. 50)

eliminate corruption in order to build a stable business setting. Local officials, on the other hand, follow their own agenda. They might be interested in the prosperity of local firms for maintaining or increasing taxes, helping out people within their relationship network, winning upcoming elections or simply personal gain (money, support, etc.). The central government and the National People's Congress are trying hard to fight corruption by passing tough anti-corruption laws and by seriously demanding their enforcement.[84] The Wuhan affair, in which senior officials fought corruption and prosecuted corrupt judges on all levels, is an excellent example of the determination of the central government to improve the situation.[85] The central government demands those improvements for various reasons: It sees the need to provide a stable business environment. Furthermore, the improvements are also a reaction to pressure from other countries and the WTO. Initiated by external pressure, the Chinese administration has realized that conflict resolution in front of courts is an important dispute-resolution and complaint mechanism that can reduce conflicts and thereby help to maintain social stability. Unsurprisingly, the Chinese population is increasingly making use of this complaint mechanism. *"[S]ome 4.4 million civil cases were filed in 2005, more than double the total a decade ago."*[86]

I would like to close this short section on corruption with a quote: *"Courts play an interesting role in the Chinese political economy in transition; they are seen as authoritative (despite problems with enforcement) but not necessarily fair."*[87]

4.3.4 Non-Disclosure and Non-Competition Agreements

Talking about problems with China's judicial system that outsourcing clients face, we should also have a short look at legal measures they employ in contracts. A very common (and necessary) aspect of outsourcing contracts are non-disclosure agreements with the provider. Those non-disclosure agreement are provisions restricting the provider from disclosing information to third parties without the permission of their clients.

The normal procedure of signing and enforcing non-disclosure agreements is as follows:

1. Service provider and client sign a confidentiality agreement.
2. The outsourcing provider signs non-disclosure agreements with all employees and third parties providing services for it.
3. If employees or third parties disclose information, they are legally punished and the customer receives financial compensation.

---

[84] See Henderson (2007, p. 155)
[85] See Henderson (2007, p. 156)
[86] See Henderson (2007, p. 154)
[87] See Clarke et al. (2005, p. 47)

If confidential information is disclosed, a couple of problems arise:

1. It is difficult to find out that information leaked at all.
2. Companies need to prove that information leaked at the service provider and not at the own firm.
3. Evidence needs to be found which proves that a particular employee disclosed information. This is particularly hard if the employee already left the firm. This is mainly a task for the service provider but without this step it is difficult to prove that the information leak was the provider's fault.
4. Even if evidence has been found, the confidentiality agreement needs to be enforced so that the provider pays compensation.

Besides non-disclosure agreements, there is another tool that outsourcing providers often employ to protect their clients, but also their own business. Companies often sign non-competition agreements with their employees. Those agreements prevent their employees to work for a competitor after they resign or get fired. Since the problems that companies face with non-disclosure agreements are similar to the ones with non-competition agreements, I would like to elaborate on non-competition agreements in the following. My interviewees reported many cases in which former employees of outsourcing providers not only disclosed information about clients but also about the internal security processes of their former employers. In some cases, they even used their old accounts to log into their former employers' systems. This is a serious security threat, especially if an employee has started working for a competitor of the outsourcing provider or a competitor of its clients. According to federal law, companies need to compensate their employees if they require them not to work for a competitor afterwards. The exact regulations concerning non-competition clauses partly depend on the jurisdiction. In Shanghai, for example, the maximum time frame that a company can require an employee not to serve another firm in the same field is three years.[88] Furthermore, the compensation companies have to pay is not clearly regulated. Some of my interviewees pay one to two months of salary, others did not pay anything, even though most companies were located in Shanghai, the same jurisdiction. It often happens that employees do not stick to them even though they signed it.[89] If a company would like to enforce a non-competition clause, new problems arise. There is no strict definition of which other companies are regarded as direct competitors and employees therefore often get around prosecution.

As for non-disclosure agreements, the main problem with non-competition agreements is to find evidence and prove the misbehavior of (former) employees. The chances to successfully plead a case are significantly higher if a company collects initial evidence before officially suing the suspect. Afterwards, a court can get more evidence, can seal computer, etc.

---

[88] That was at least the current situation when I conducted research.
[89] Here again, theory and practice diverge.

   The main problem of collecting evidence remains. If it is necessary to collect it before suing the suspect, it needs to be done without involving law enforcement agencies.[90] One way to collect the evidence is to hire a private or commercial investigator. We will take a look at this option in the following.

4.3.5 Private Investigation

As we just saw, finding evidence that proves that a non-disclosure or a non-competition agreement was broken or intellectual property rights violated is one of the major problems of the Chinese legal system.

   In order to find evidence (that can be presented in front of a court), attorneys often hire private investigators. Especially in China, many companies would like to make use of those services because they are afraid of bribery and tight personal relations between the natural person or managers of the legal entity they would like to sue and law enforcement agencies which should examine their case. In trademark disputes, for example, it still happens that courts and law enforcement agencies warn the accused so that they can hide evidence before law enforcement pretends to investigate the case. Searches therefore discover no evidence. A major problem that companies looking for investigation services face is that it is impossible to get a business license as a private investigator in China. I talked to various lawyers specialized in this field but none of them could answer the question whether private investigation is officially forbidden or if the government just does not grant any licenses. It seems to be within the gray area. In order to explain the current situation I would like to refer to a firm offering private investigation services. This is an excerpt of its response:[91]

   > 80% of the investigation firms register *consulting services* as their business scope.[92] [. . .] Generally speaking, the service provided by the consulting companies is a category of investigation as well and is legal. In China, individuals are entitled the right to do investigation work. In the light of Chinese culture and from the legal angle, investigation is the process of information observation, learning, collection and analysis without any enforcement while the real detective is endowed with the rights of search, tracing, inquest and interview following legal procedures. Therefore, in compliance with the laws in China, there is no detective in non-governmental circles.

---

[90] There is another reason for collecting the evidence, as will will see in the next section.

[91] Statements from all other interviewees confirmed this interpretation. It was not possible to receive any official statement from a Chinese government body.

[92] I was told that there are about 1,000 companies in China that offer investigation services and are registered as consulting companies. Most others, which are not registered as consulting firms, seem to register in the field of marketing or public relations.

This told it becomes obvious that there are private investigation firms in China. However, they are not able to get a business registration as a *private investigator* from the *State Administration of Industry and Commerce* (SAIC). If those companies cannot obtain a business registration, but are conducting private investigations anyway, they operate outside the boundaries of their original registration. As SAIC does not provide business registrations for private investigators, they can revoke the business registration of those companies.[93]

Another problem one is confronted with when hiring an investigation firm is that the evidence those firms collect cannot officially be used in court against the defendant. It could be used, theoretically, if the court authorizes a "consulting firm" to investigate and cooperate with law enforcement agencies. However, this circumvents secret investigation and raises again the problem of corrupt courts that might warn the accused.

Companies depend on an immature legal system with corrupt judiciary. Without the option to hire private investigators and to use their investigation results in front of a court, it is extremely hard to find evidence. Breeches of legal agreements are therefore hard to prove. Legal disputes are often settled in the favor of the company with the best relation to local courts.

4.4 Infrastructure

Besides China's immature legal system, there are other environmental factors that influence outsourcing activities. In the following, I focus on two of them: *Infrastructure* and *Technology*. I give an introduction to Chinese cryptography regulation, describe China's telecommunication infrastructure[94] and provide an overview of its telecommunication market. At the end, I discuss the role that media plays for information security and the outsourcing market.

4.4.1 Cryptography Regulations

Today's information security world is unthinkable without cryptographic tools. Cryptographic algorithms were one of the first research areas in the field of information security. Research in this field was strongly supported by governments and the military. The encryption of messages must not be the only security measure applied by a company but a security concept always partially relies on cryptography. Some countries, including China, impose restrictions on encryption devices so that their security agencies can decipher

---

[93] This usually does not happen because people setting up investigation firms are often former high-ranking police or military officials with good relations.
[94] This description includes a short introduction to China's Great Firewall.

and monitor communication.[95] However, the exact situation regarding cryptography restrictions is unclear.[96]

The *Crypto Law Survey* by Bert-Jaap Koops is probably the most comprehensive description of cryptography regulations.[97] But as I said before, at least in China, the legal situation concerning the import, export, use and development of products with cryptographic functions is extremely hard to clarify and even the Crypto Law Survey does not provide detailed information. Many of my interviewees complained about this situation because they were concerned whether or not they operated within the legal framework. The following explanations are based on the *Crypto Law Survey* (Koops, 2008) and *Using Encryption Internationally* by Diane E. Levine.[98]

The State Council Order No. 273, *Commercial Use Password Management Regulations*, published in October 1999, is the current regulation that restricts the use of cryptography in China. It regulates on two levels, the import and export of crypto products as well as manufacturing and use within China. Import and export of crypto products requires a license by the State Encryption Management Commission (SEMC) if encryption and decryption are core function of the device.[99] Key escrow is not demanded by the SEMC. However, the latter two exceptions (only for devices with crypto as a core function and no key escrow) might only apply to pre-2000 products which leaves the question how newer products are dealt with. As I said, besides import and export, also the development and use of crypto products is restricted in China. Manufacturers need to register and obtain approval from the SEMC for every product. Individuals as well as organizations are only allowed to use products approved by the the SEMC.[100] New rules seem to require the registration of any use of commercial encryption products.[101] According to an article at Wired with the headline *Chinese Crypto Regs? 'Whatever'*, also individuals using desktop software with encryption functions (almost any Internet user) need to register based on the new rules.[102] However, not even Chinese and

---

[95] See Ulrich, Chacko, and Sayo (2004, p. 32 f.) in Sayo, Chacko, and Pradhan (2004)

[96] For an analysis of global cryptography legislation, see Aljifri and Navarro (2003). Concerning China, Aljifri and Navarro only refer to the *Commercial Use Password Management Regulations*, which is also discussed in the *Crypto Law Survey* (see below).

[97] The Crypto Law Survey is available at `http://rechten.uvt.nl/koops/cryptolaw/cls2.htm#prc` (Koops, 2008). [19.07.2008]

[98] See Levine (2002, p. 50.7 f.) in Bosworth and Kabay (2002)

[99] Mobile phones, browsers, etc. are therefore exempted.

[100] According to Levine (2002, p. 50.7 f.), Chinese firms are not allowed to use any foreign cryptographic software.

[101] Only embassies and consulates are exempt from this requirement. Germany's representations can therefore import and use SINA products developed by the German security firm *secunet Security Networks AG*.

[102] See `http://www.wired.com/politics/law/news/2000/01/33992` [09.07.2008]

foreign companies cared about the deadline and almost nobody showed up to register their usage.

This operation in a gray area, being required to register their use of crypto devices but not complying with the regulation, worried some of my interviewees.[103] They were afraid of penalties but even more worried about the confiscation of their or their outsourcing providers' crypto devices and servers. Two interviewees told me that they needed to use German crypto products due to their companies' security policies. Instead of importing them officially, they just took the hardware with them on the plane when traveling from Germany to China and downloaded encryption software from their German servers. Another interviewee told me that he wanted to register their use of cryptographic products but did not manage to. He asked many security experts and even talked to government officials at SEMC about current legislation and how to comply with it but never received clear answers. After a couple of months, he received a registration form from a colleague and sent it to SEMC but never received any reply, not to mention a letter of approval. Even though there are no public cases of prosecution and confiscation due to unapproved crypto use, security managers perceive the unclear legal situation as a risk that might turn into a security threat for outsourcing in the near future.

Besides the restriction of import, export and use of crypto products, China tries to influence international encryption standards. An excellent example of China's efforts in this field is the WAPI standard. It also provides another insight into how companies react to the regulation of cryptography. WAPI is a Chinese national standard for wireless networking whose encryption algorithm was classified as a Chinese state secret for a long time. Its development was primarily driven by the Chinese government which repeatedly tried to turn it into an international standard.[104] The Chinese government argued that WAPI closes security loopholes in 802.11 and that it would be cheaper because it is a local product.[105] Critics argue that the classified encryption algorithm (SMS4) might include a backdoor that can be used for decrypting messages by the Chinese government. Even if that was not the case, the algorithm had not been peer reviewed by the international security community and could therefore not be regarded as secure. Other voices said that WAPI was merely a tool to gain profit because all companies that wanted to offer wireless networking products had to cooperate with a few Chinese firms that had access to all necessary information.[106]

---

[103] Some others did not care about it at all because they believed the regulation would never be enforced. The opinion was split quite equally between all the people I talked to about this issue.

[104] A detailed observation of China's efforts to submit WAPI as an international standard at IEEE are described in DeLacey, Herman, Kiron, Lerner, and Lo (2006).

[105] See `http://news.xinhuanet.com/english/2006-03/05/content_4262089.htm` [19.07.2008]

[106] See DeLacey et al. (2006, p. 11)

Intense protests from international firms were started when Chinese government agencies declared in May 2003 that *"by December all wireless devices sold or imported into China needed to incorporate the WAPI technology"*.[107] About a year later, in April 2004, some members of the international standardization community considered it to be the 'mortal blow' to WAPI when high-level trade talks persuaded China to suspend this regulation indefinitely.[108] The Chinese government, on the other hand, only saw this suspension as a way to turn WAPI into an international standard after submitting it to JTC1 (ISO/IEC Joint Technical Committee 1) for international adoption. This request was declined in September and again in December 2005 because SMS4 (the crypto algorithm used in WAPI) was inaccessible for non-Chinese parties and had not been reviewed by the international community.[109] China responded in two ways: It declassified the SMS4 algorithm in January 2006 and at the same time *"directed all government purchases to be WAPI-compatible"*.[110] Two months later, an official vote at ISO/IEC (which was criticized as unfair by Chinese officials and researchers) supported 802.11i by a large margin over WAPI as the new international standard.

Today, WAPI devices are officially preferred by the Chinese government but in practice they do not play any relevant role. Especially in the non-governmental market almost all devices are used with other (internationally accepted) security algorithms. The WAPI case illustrates the way companies handle cryptography in China. They disrespect government recommendations and even legislation because those are not enforced up to now. However, the reaction of the Chinese government to this 'illegal behavior' is hard to predict.

4.4.2 Internet Filtering: The Great Firewall of China

China has always tightly controlled the spread of news. The government believes that social and political stability can only be assured by filtering the information that is passed on to common citizens. Article 57 of the *Telecommunications Regulations of People's Republic of China* lists the kind of content that is deemed inappropriate and therefore banned.[111,112]

No organization or individual may use telecommunications networks to produce, reproduce, disseminate or transmit information with content that:

1. *opposes the fundamental principles determined in the Constitution;*
2. *compromises State security, discloses State secrets, subverts State power or damages national unity;*

---

[107] See DeLacey et al. (2006, p. 11)
[108] See Lin-Liu (2004, p. 16 f.)
[109] See DeLacey et al. (2006, p. 22 f.)
[110] See DeLacey et al. (2006, p. 14)
[111] See Ministry of Information Industry, People's Republic of China (2000)
[112] For more information, see, for example, Wacker (2003, p. 62) in Hughes and Wacker (2003)

3. *harms the dignity or interests of the State;*
4. *incites ethnic hatred or racial discrimination or damages inter-ethnic unity;*
5. *sabotages State religious policy or propagates heretical teachings or feudal superstitions;*
6. *disseminates rumours, disturbs social order or disrupts social stability;*
7. *propagates obscenity, pornography, gambling, violence, murder or fear or incites the commission of crimes;*
8. *insults or slanders a third party or infringes upon the lawful rights and interests of a third party; or*
9. *includes other content prohibited by laws or administrative regulations.*[113]

Any information that involves content which fits into one of the categories above is forbidden and the Chinese government tries to filter it, partly by using its *Great Firewall*. In the offline world, news agencies have been state-owned and thereby only published censored information. Today, with the spread of computers and Internet connectivity, the government has more and more problems to stop unwanted information from spreading across the country. Especially the rise of decentralized publishing in form of blogs is causing problems because the government does not have any direct control over bloggers, especially if they live or publish in foreign countries.[114] Within China, Internet dissidents can be prosecuted, servers confiscated and Internet connections cut, but information published cannot be stopped from spreading with legal means. Therefore, the Chinese government resorted to technical solutions and built the *Great Firewall*, probably the largest content filter in the world.[115,116]

The Great Firewall is a large 'packet filter' installed at China's national borders.[117] It filters content based on keywords that are deemed inappropriate

---

[113] See Ministry of Information Industry, People's Republic of China (2000)

[114] Blogs are difficult to censor but they also exhibit another problem for the Chinese government. Like other new tools on the Internet, blogs offer a new way of information exchange. Communication is not necessarily one-way anymore but readers can reply to articles and spin off new discussions. People are meant to participate in blogs through comments. This might also lead to an increase in the formation or political groups and the participation in political discussions in the offline world.

[115] The 2008 Annual Report by *Reporters Without Borders* summarizes China's censorship activities. It also contains a short paragraph on China's Great Firewall. See Reporters Without Borders (2008)

[116] RAND's National Security Research Division published a profound analysis of the political use of the Internet by Chinese dissidents and Beijing's counterstrategies. See Chase and Mulvenon (2002)

[117] This perimeter firewall, which is often referred to as the Great Firewall, is part of an enormous range of activities focusing on censorship and surveillance. All activities are grouped in the *Golden Shield Project*. See Walton (2001). Since it is rather a nickname than the real name of a project, there is no common

by the Chinese government.[118] Search requests based on these keywords are not transmitted and connections to websites containing 'inappropriate' content are blocked. Since the Great Firewall is installed at China's borders, it has some limitations. As long as the traffic stays within China, the Great Firewall does not seem to interfere.[119] If a company and its outsourcing provider are both within China, the Great Firewall therefore does not raise any bigger problems. However, China applies other filter methods that also affect traffic within China and therefore also have an impact on domestic outsourcing activities.

There are at least four known methods that are used by the Chinese government to filter unsolicited content:[120,121] *IP Address Filter*, *Manipulation of the Domain Name System*, *Help by Major Search Engines* and *Keyword-based Web Browsing Filter*. During the time I lived in China, I could verify the application of all of those methods. In the following, I will go through those techniques and link them to the topic of this thesis, security risks related to outsourcing in China.

IP Address Filters are used for filtering single IP addresses or entire ranges of IP addresses based on a list that is filled by China's Internet police.[122] If a web server provides 'inappropriate' content, its IP address is added to the list and all connection requests to this machine are blocked. Those block lists are used for filtering at the borders, as part of China's Great Firewall, but their use also seems to be mandatory for a wide range of Internet service providers. Therefore, this method also works if both server and user are located within China. For outsourcing activities, but of course also for private and business Internet use, those IP-based block lists lead to a couple of serious problems. Filtering entire hosts based on IP addresses renders all services on these hosts unavailable. If one website on a physical server is blocked, all other

---

understanding of what China's *Great Firewall* is. I will use this term as a reference to the content filter installed at China's national borders.

[118] Companies like Cisco have been criticized because they supply the technology which is used for China's censoring efforts.

[119] There might be certain peering locations, for example when data flows from China Telecom's into China Netcom's network) that are filtered as well. Up to now, very little is known about the Great Firewall but it seems to be installed solely at the perimeter – when traffic flows between China's and other countries' infrastructure.

[120] In 2003, Jonathan Zittrain and Benjamin Edelman conducted a research project on China's filtering activities. See Zittrain and Edelman (2003). The OpenNet Initiative (ONI) at Harvard University's Berkman Center still collects data on global Internet filtering. See `http://opennet.net/`

[121] See also Clayton, Murdoch, and Watson (2006) and Wolfgarten (2006). Most descriptions below are based on these publications, personal experiences with and tests of Chinese filtering measures.

[122] Various news sources published a figure of 30,000 employees responsible for controlling Internet activities in China. However, the real number is unknown. The IP address filters might also be filled by automated methods. Keeping those filters up-to-date is a major problem and it is unclear how it is addressed.

services (including websites) on this host become unavailable as well because
the entire machine is blocked. For small outsourcing tasks, many companies
use virtual servers (often without own IP addresses) and a single website with
inappropriate content can lead to the unavailability of all customers' services
on this machine.[123] This problem is even more serious if not a single IP address
but a whole range of addresses is blocked. Since also ISPs seem to be forced to
use block lists compiled by the Chinese administration, it does not matter if
only one party (client or outsourcing provider) or both are located in China.
The availability of the desired services cannot be guaranteed.

The second filtering method is *manipulating the Domain Name System
(DNS)*. The purpose of the DNS is to resolve host names to IP addresses.[124]
The Chinese government seems to use two different ways of manipulating the
resolution of host names. The first method is *DNS Redirection* (also called
DNS poisoning or *DNS hijacking*). This means that Chinese DNS servers in-
tentionally resolve host names to wrong IP addresses. Thereby, the Chinese
government can redirect traffic to own servers or into nirvana. Those servers
either serve a notification page (for example that one wanted to access inap-
propriate content), do not serve any web site at all or serve a replacement of
the original web site.[125] The second measure is to entirely stop host name res-
olution for specific host names. Wolfgarten found that some host names were
not resolved at all and requests for blocked domain names often resulted in
SERVFAIL or timeout errors.[126] This also renders the entire host (or domain)
unavailable. There is a third method with the same result which 'manipulates'
the DNS but uses the first measure we discussed, IP address filtering. Specific
DNS servers seem to be filtered based on their IP addresses. All services of
the domains resolved by these DNS server are thereby unavailable because IP
addresses cannot be resolved. All of those techniques are extremely easy to im-
plement. As well as IP address filtering, these measures are not only deployed
at China's borders but the Chinese administration also relies on the coopera-
tion of China's ISPs for filtering within the country. Since DNS manipulation
does not lead to overblocking, it is less likely to cause any severe outsourc-
ing problems. Furthermore, it can easily be circumvented.[127] However, two

---

[123] Research by Benjamin Edelman shows that in 2003 87.3 percent of active com,
net and org websites shared their IP address with other sites (more than two-third
even with 50 others or more). See Edelman (2003). This does not say much about
commercial use of servers but gives an idea of how common address sharing is.
Server sharing is even more prevalent.

[124] The host name *www.tu-berlin.de* is for example currently resolved to
130.149.4.134.

[125] Of course, this method works in exactly the same manner for other services besides
http.

[126] See Wolfgarten (2006)

[127] One can simply use another DNS server which is not controlled by the Chinese
administration. When I tried this countermeasure, some DNS servers were un-
reachable (but only a very few of those I tested). However, I could reach them

interviewees reported problems they encountered. One described that their outsourcing provider's servers were not reachable for a few hours because domain names could not be resolved. By resolving those domain names manually, the problem was solved and after a few hours the system worked again. However, if they had deployed their web site or web services on those servers, customers would not have been able to reach them. Another interviewee told me that the host name of one of their hosts running a secure shell (SSH) server was resolved incorrectly. When an IT admin tried to login on the machine, another server responded, also running SSH. This particular admin was well-trained and realized that he was connecting to the wrong server because the key's fingerprint did not fit.[128] After about two days, the host name resolution was back to normal again. The company never found out if the wrong resolution was intentional, maybe preparing a man-in-the-middle attack, or if configuration files on their ISP's DNS servers were corrupt due to a mistake. DNS manipulation can be used for denial of service attacks or for preparing other attacks but the filtering of particular domain names by the Chinese administration normally does not cause any security risks.

Surprisingly, the third filtering method is supported and even enabled by foreign companies. Major players in the search engine market like Google, Yahoo and Microsoft acknowledge that they filter content based on keywords in order to comply with Chinese legislation.[129,130] Thereby web pages that serve unsolicited content are not displayed in the list of search results. The help of major search engines was hardest to verify because their ranking algorithms are unknown. However, the use of the same search query lead to another list of search results using a German and a Chinese IP address.[131] Since this behavior does not cause any security threats,[132] this method is not discussed any further.

---

from German IP addresses. It is unclear if they were blocked based on their IP address or if other connection problems occurred. For the Chinese administration, it would make more sense to entirely block all outgoing DNS requests than to filter single IP addresses.

[128] This shows how important security sensitive (IT) personnel is. Without this security-aware IT admin, the company's server could have been compromised.

[129] Especially Google was strongly criticized for helping the Chinese government because this seems to infringe its motto *Don't be evil*.

[130] Of course, the same is true for Chinese search engines like the market leader Baidu, but also smaller ones like Yisou. See OpenNet Initiative (2005)

[131] Furthermore, when searching for keywords that are likely to be filtered, google.cn shows a short notice at the bottom of the search page that results are filtered due to Chinese laws and regulations.

[132] If one regards the delisting in search engines as a threat because people do not find the site anymore (unavailability), it can be seen as security-relevant. However, it does not threaten confidentiality, integrity or availability of the data itself.

The fourth method is probably the most prominent one because it is most obvious to normal Internet users.[133] It can be described as a *keyword based web browsing filter*. It is the technique that is often described as the Great Firewall. It is a filter that searches for predefined keywords in URLs and HTML. If an unsolicited keyword is found, the connection is dropped by repeatedly sending TCP resets (RST packets).[134] Furthermore, the connection between destination host and the user's computer is blocked for a short period of time (usually a couple of minutes). This content filter seems to be entirely symmetrical and shows the same behavior accessing information abroad from within China or the other way around. It seems to be solely deployed at China's borders and not within the country. Since all traffic needs to be directed through proxy servers which scan for unsolicited content, it would be extremely costly to also filter all traffic within China. Even the filters at the borders seem to be overstrained sometimes. This can be seen as outsourcing-relevant. Since many companies need to access data abroad[135] and for some applications large data volumes need to be transferred, services might become unusable if those filters are overloaded. If a company's corporate website is hosted outside of China and accessed from within (or the other way around), it might be filtered due to the use of unwanted words or a misconfiguration of the filter. However, because this measure mainly affects web sites[136] and only causes problems when one party is outside of China, it is almost irrelevant for this thesis.

There are various ways to get around China's Great Firewall and its other filtering measures in order to access censored information. Easy methods that can be applied by end users are the use of proxy servers, virtual private networks (VPN) or Tor.[137,138] Since many companies use virtual private net-

---

[133] The unavailability of particular web sites over a long period of time is obvious as well. However, the total unavailability could also be caused by problems on the destination's side. Furthermore, concerning this filtering measure, the user can himself test which kind of content is censored by Chinese administration.

[134] Another method is to forge SYN/ACK packets on the firewall with an incorrect sequence number. If this answer arrives before the original reply, the connection cannot be established because the handshake fails. This measure is described in Clayton et al. (2006).

[135] One reason could be that the outsourcing provider is in China and the client has offices abroad. Another one is that some data is still at the headquarter of the client or another data center in another country and needs to be accessed.

[136] The content filter might also be deployed for other services (like unencrypted e-mails). However, there is no information available on the filtering of other services.

[137] Tor is a software project that protects its users from traffic analysis. It uses a distributed, anonymous network and routes requests through the network in an ever-changing and unpredictable way. Furthermore, all traffic that is relayed through the network is being encrypted, except the last hop, the data exchange with the final destination. See `http://www.torproject.org/`

[138] There is another rather tricky way to circumvent the Great Firewall (at least its filtering method which is based on sending RST packets). As described before, once triggered (by particular keywords), the firewall sends TCP resets and

works for accessing data at their headquarters, their subsidiaries or at their outsourcing providers' data center (which all might be in different countries), the content filtering function of the Great Firewall does not play a major role for them. Most employees do not search for words that might be filtered and those websites that are fully blocked over a longer period of time are usually not the ones that need to be visited work-related. Therefore, the content filtering function of the firewall does not matter to many employees. Most of them probably not even realize that certain websites and terms are blocked. My interviewees were mainly concerned about the first two measures, IP address filtering and manipulation of the DNS because those measures can cause serious security threats.

4.4.3 Excursus: China's Internet Infrastructure

After this discussion of China's efforts to censor and control Internet traffic, I would like to give a very short overview of China's overall Internet infrastructure. Especially concerning its network links to the rest of the world, there are some interesting insights that I will briefly present in the following.

Since early computer networks (which later turned into the Internet) were sponsored by the military, redundancy and reliability have always been core design principles. Still today, the networks that form the Internet are built with a focus on redundancy. Most countries try to avoid choke points because traffic should be rerouted as quickly and transparent as possible when single routes fail. The network design looks very different in China. The Chinese 'intranet' is linked to the rest of the world at a very few choke points: *"the Beijing-Qingdao-Tianjin area in the north, where cables come in from Japan; Shanghai on the central coast, where they also come from Japan; and Guangzhou in the south, where they come from Hong Kong"*[139] There are overland cables through India and Russia as well as satellite uplinks but both play a negligible role because very little traffic is routed through those con-

---

afterwards relies on the endpoints to drop the connection accordingly. If an endpoint does not implement the TCP protocol in a standard-compliant manner or is tweaked so that RST packets are simply ignored, the requested website is transferred without any problems. Clayton et al. (2006) achieved this behavior by simply adding a rule to the packet filter (iptables in their case) which dropped all RST packets. One major drawback of this method which makes it less useful in reality is that both endpoints must be manipulated. If one had full access to both endpoints, there would be more effective ways two circumvent the firewall and protect against traffic analysis at the same time. However, the experiment of Clayton and his colleagues provides valuable insights into the functioning of the Great Firewall.

[139] See Fallows (2008). The *China Internet Network Information Center (CNNIC)* regularly publishes a map of Internet Connections in China. This map also highlights those three choke points: Beijing, Shanghai and Guangzhou. See CNNIC (2006)

nections.[140] The design of the network with three major choke points has a valuable advantage for the Chinese administration. Those choke point make it easier to filter traffic than if many possible routes would exist. The Great Firewall only needs to be installed and administered at those few locations and almost all traffic can be filtered there. On the other hand, it also makes the network more fragile.

When a series of earthquakes hit the Luzon Strait in front of Taiwan's coast in December 2006, a large problem with the network design in Asia (and in China in particular) was revealed. Since a large number of submarine cables connecting Asian countries with each other and with the rest of the world run through the Bashi Channel in the Luzon Strait, this particular spot can be seen as a huge choke point. The earthquake damaged many of those cables and the Asian telephone and data network collapsed. China was one of the countries that were cut off from the rest of the world.[141] This incident revealed the fragility of the Asian Internet infrastructure and China's infrastructure in particular.[142,143] Service providers announced that they would reroute traffic via overland and satellite routes. However, those could not cope with the dramatic rise of traffic. Traffic in most Asian countries was rerouted rather quickly but China was almost fully cut off for weeks. Many bloggers even complained after more than a month that their Internet speed was still not back to normal. The choke points in the Chinese infrastructure, which are very convenient for filtering all in- and outgoing traffic, turned out to be a severe problem. Since in normal times very little traffic is transmitted via other links (like the overland route through Russia) compared to the three large data exchange points, the infrastructure there is not able to handle such a steep increase in traffic volume. The Chinese infrastructure is not built to react to rapid changes and to rebalance traffic by routing through other paths. Furthermore, it is likely that not only the network itself, including the routing infrastructure, but also the Chinese Great Firewall was overstrained because it had to handle a lot more traffic than normal at unusual routes.

This example illustrates how fragile the Chinese Internet infrastructure still is. It highlights what can happen in cases of natural disasters. The connection at the few choke points that connect China with the rest of the world can be fully interrupted. Natural disasters are only one example for possible incidents that might cause such an outage. If the political conflict with Taiwan escalated, the government of the People's Republic might order to cut off Taiwan's links to other countries. The same might also happen the other way around. Since most submarine cables lie in front of Taiwan's coast, the military of the Republic of China could try to destroy Internet connectivity

---

[140] See Wolfe (2007)

[141] See, for example, `http://news.netcraft.com/archives/2006/12/27/taiwan_earthquake_limits_access_to_chinese_hosts.html`

[142] See Wolfe (2007)

[143] For a detailed description of the problem, see, for example, `http://blog.cytrap.eu/?p=153` and `http://blog.cytrap.eu/?p=160`.

of the People's Republic of China as well. How fragile China's infrastructure really is can not only be observed when special incidents occur, it can also be studied in everyday life. Many people and companies situated in China complain that the bandwidth to foreign servers is constantly changing but often poor. The Great Firewall of China seems to be at its capacity limit and Chinese Internet users experience problems accessing foreign web sites, especially at peak times. Furthermore, latency is another serious problem. Since most traffic is routed via the United States, especially accessing servers in Europe is troublesome. Interestingly, the same is true for most traffic to Taiwan. It is also routed to the United States and back to Asia again. Missing redundancy, due to only a few choke point, congestion of the Great Firewall and inefficient routing between China and the rest of the world, are serious weaknesses of the Chinese infrastructure.

This fragility poses a risk from an economic but also from a security perspective. A longer outage of telephone and Internet connections would have a disastrous impact. Since this thesis mainly focuses on outsourcing activities within China (both parties, client and provider, are located within China), the influence from a security point of view is not dramatic but also by far not negligible. As mentioned earlier, outsourcing activities cannot be viewed purely limited to what happens within China. An Internet connection to destinations outside of China is indispensable. Security updates must be downloaded from servers outside of China, information must be exchanged with people abroad, some servers that are necessary for daily operating might be located in other countries, etc. If the connection does not function properly, this is a security risk for the outsourcing client and its service provider.

4.4.4 China's Telecommunication Market

China's telecommunication industry is one of the most restricted business sectors. The limited number of providers leads to minor problems. Due to legal regulations, there are only three large telecommunication operators in China that offer fixed line telecommunication services.[144] Two of those, China Telecom and China Netcom dominate the market and serve almost all fixed line phones. The third provider, China Railcom (which is also known as China Tietong Communications) is secondary due to its size. It is not entirely insignificant because it works closely with cable television providers and therefore does not need own telecommunication cables for the last mile.

The market I just described was the distribution at the time when I conducted research for this thesis in China (primarily in autumn 2006). However, the Chinese telecommunication market is undergoing rapid and substantial changes. On May 23rd 2008, mobile phone operator China Mobile announced a takeover of the smallest of the three fixed line operators, China Railcom,

---

[144] Furthermore, the are mobile phone operators and satellite communication services.

and thereby started the process of reorganization.[145] Furthermore, and more importantly, China Netcom and China Unicom will merge in order to react to a convergence of fixed line and mobile phone services.[146] China Unicom will at the same time sell its CDMA network to China Telecom but the new merger will keep its GSM mobile network.[147] In contrast to the old structure, all providers will be able to provide fixed line and mobile phone services after the completion of the restructuring. China would like to use this step in order to improve competitiveness of its providers in the industry. Xi Guohua, the vice-minister of industry and informatization, said at a press conference that the process will take about six month and that *"China will issue third-generation mobile telephony licenses once the restructuring process has been completed"*.[148]

Even though the restructuring of the telecommunication sector is a giant change, I would like to present the problems which I found by interviewing experts in China before the reorganization. Changes in the telecommunication sector do not render my research results invalid because the problems exist on a deeper level and will persist. Most problems are part of the market regulation[149] and are rooted in China's infrastructure and its telecommunication personnel. They are therefore likely to survive the restructuring of the market and will not vanish because of new shareholders.

Before 2002, China Telecom had a quasi-monopoly on the market for landline subscribers (99 %).[150] In May 2002, China Telecom's landline business was split into the southern and western provinces, which remained at China Telecom, and the northern provinces which were handed over to China Netcom.[151] At the time of conducting the interviews (autumn 2006), China Telecom and China Netcom still had a quasi-monopoly on the landline market which was divided regionally amongst those two.[152,153] This exhibited and probably still exhibits a couple of problems that I describe in the following.

---

[145] See, for example, `http://www.bloomberg.com/apps/news?pid=20601087&sid=a_ryexF4S2NI` [23.07.2008] or `http://www.interfax.cn/news/news/2662/` [23.07.2008]

[146] See `http://www.china-netcom.com/eng/ir/press/p080602.pdf` [23.07.2008] and `http://www.chinaunicom.com.hk/en/press/pressrelease/news.html?id=4581` [23.07.2008]

[147] See `http://www.cnbc.com/id/25714495/` [23.07.2008]

[148] See `http://www.cnbc.com/id/25714495/` [23.07.2008]

[149] The telecommunication market is opening up, also due to China's accession to the WTO. However, it can still be regarded as one of the most restricted sectors in China. See, for example, Ure (2002)

[150] See Sautedé (2002, p. 40)

[151] China Netcom was only founded three years before. The decision that is could take over China Telecom's business was strongly supported by Jiang Mianheng, Jiang Zemin's son. See Sautedé (2002, p. 41)

[152] As I mentioned earlier, there was also China Railcom offering landline phone services. However, China Railcom could only acquire a very small market share.

[153] See Brahm (2002, p. 203)

Even though China Telecom and China Netcom divided the market regionally, they were starting to fish in each others markets. Furthermore, due to the forced breakup of China Telecom's business, the relationship between both companies was fierce. They saw each other as competitors and also operated accordingly. This led to problems concerning the data exchange between their customers because – that is at least what many interviewees assumed – the networks were separated artificially and peering was deteriorated intentionally. This was an immense problem for companies having their headquarters or subsidiaries in southern provinces and their data center in the north, or the other way around. In those cases, the network connection and thereby the data exchange was slow, sometimes even too slow to properly use data-intense applications over the network. Some interviewees even reported that the connection was repeatedly unavailable for hours. Those problems could hardly be solved because Internet connections were only offered by either China Telecom or China Netcom, depending on the region.[154] This also made fallback solutions with backup lines in case of network problems at one operator's network difficult.[155] Outsourcing clients had to install dial-up connections or satellite uplinks in order to assure the availability of the network connection to their outsourcing providers' data centers. Implementing redundant data connections was especially difficult in rural areas. Companies building their factories or local subsidies in undeveloped areas due to lower real estate prices experienced that either no data connection was available at all or that the laying of data cables took much longer than anticipated. In those areas, redundant connections were almost impossible to realize. Companies that developed previously uninhabited areas suffered the problem that their only data connection, which they could use after a lot of trouble with their operators, was often unavailable due to new constructions around their site. Construction workers accidentally cut their cables and the operator could send service technicians only after a few hours had passed. In some cases, it even took days for the technician to arrive. Well-trained technical personnel can be regarded as a problem that telecommunication operators in rural areas still face. Professionals move to the coast in order to work in cities like Shanghai, Beijing, Dalian, Qingdao or even Hong Kong. As a consequence, manufacturers with their production sites in rural areas suffer because their network problems are not quickly resolved and because they do not have the choice to change operators.[156]

Even after the merger of China's telecommunication operators, there will be two main providers of fixed line servies – China Netcom/China Unicom and China Telecom (with China Unicom's GSM network). China Mobile (in-

---

[154] In some cities, both operators offered their services but the division according to provinces was the normal case.

[155] Some data centers in China, even two years ago, already had connections served by both China Telecom and China Netcom. However, this setting was pretty rare.

[156] Two companies I talked to decided to totally resort to satellite uplinks to address this issue.

cluding China Railcom) will still play a less important role. It is uncertain how China will address these issues. Even a deregulation of the telecommunication sector will not bring the desired results immediately because the last mile cannot be covered by new operators and because many problems are due to poor infrastructure and personnel. It seems likely that those problems will be addressed by a more intense use of wireless uplinks.

4.5 Media and Image

One of the big drivers of information security in Western countries is the increased media coverage of security incidents. The media presence of information security topics is like a wave. Some topics show up again and again, others are always present. In the United States and in Europe, information security became omnipresent in the media in the last couple of years. There is hardly any day without news about worms, viruses, phishing and pharming, even in non-IT publications. This increase of media coverage got three positive effects on information security: *Influencing Legislation*, *Fear of Image Loss* and *Sensitization of Employees*.

4.5.1 Influencing Legislation

Media coverage of security and privacy incidents raise the awareness of citizens. This can lead to an increase of pressure on the administration to enact security and privacy laws. Without this pressure, governments and intelligence services would develop and implement new surveillance techniques and neglect privacy regulations. Many security researchers argue that those investigation technologies create backdoors that can not only be used by the state but also by attackers. On the other hand, the pressure can support new laws that have a positive impact on information security. They can inject the topic into the minds of managers. The most prominent example of legislation with such an effect is probably the U.S. American *Sarbanes-Oxley Act (SOX)*.[157] It was implemented as a direct response to corporate scandals like Enron, Tyco International and WorldCom. Whether its impact on security was home-made by audit and consulting firms or resulted from the legislation itself is debatable. Nevertheless, it raised security awareness at the management level and therefore can be seen as an important driver for information security, at least for all companies that are listed at the American stock market. Similar legislation has been established in many other countries. Extensive media coverage of security incidents and security (and privacy) relevant legislation can therefore be regarded as a driver for information security.

---

[157] See SOX (2002)

4.5.2 Fear of Image Loss

Most companies are afraid of a loss of reputation. If Western companies experience a major security breach, the media is likely to report about it. This is especially true for companies working in the financial industry and other knowledge-intense firms as well as for companies storing sensitive customer data. During a study in 2005, I identified the media and its recent interest in information security issues as one of the main drivers of corporate information security in Germany.[158] A participant of that study, a security manager of a financial institution, describes the force of media as follows:

> The fear of image loss is one of the main drivers of security activities. From a business management perspective, one would not do anything against phishing but rather insure against the risk. However, this kind of flexible response does not work in Germany. The customer has to see (in order to believe) that a company mitigates the risk and secures its operations.

Even though this pushes companies towards implementing security barriers which Bruce Schneier would describe as *Security Theater*,[159] it also forces companies to rethink and harden their security concepts. In order to understand how media coverage influences information security, we should have a short look at the economic rationale behind information security. Since one does not generate money with a higher level of security and security measures are only deployed for lowering risks, the costs that a security breach entails (and the likelihood of this incident happening) are most important for risk management. A major problem that risk managers face is that it is extremely hard to measure the overall cost of a media report about a security problem because it leads to *direct* but also *indirect costs*. The cost of fixing the vulnerability and compensating those that suffered the security breach can be described a *direct costs*. Indirect costs are costs resulting from the loss of reputation.[160] This loss might affect existing and potential customers, suppliers,

---

[158] See Glaser (2005, p. 48 ff)

[159] Security Theater is defined by Bruce Schneier as *"palliative security measures that only make people feel more secure"*. See Schneier (2008)

[160] Problems with the estimation of costs due to a loss of reputation are one of the main problems for calculating the *Return on Security Investment (ROSI)*. This can lead into two directions. Some companies spend incredible sums on security measures because they are afraid of the unknown outcome of a report about security breaches. On the other hand, it hinders security managers to retrieve budgets, especially for organizational measures, because they cannot prove that the money is well-spent. In *Information Security and Knowledge Management: Solutions Through Analogies?* (Glaser and Pallas, 2007), Frank Pallas and I analyze this problem and propose to look at other disciplines to see if there are *self-optimizing* approaches, like market mechanisms, that can solve the problem of ROSI calculation.

cooperating firms etc. to reconsider their business activities conducted with the attacked firm.

Since Chinese media does not report about security incidents, the fear of image loss plays an insignificant role for raising the information security level in China.

4.5.3 Sensitization of Employees

As I mentioned before, information security is omnipresent in the media to-day. News about malware and data privacy theft appear in all kinds of media channels and are not focused on IT professionals but directed at a mass audience. This presence makes employees think about information security and raises their awareness. Security breaches become part of their daily life and they slowly become aware that security incidents are not only happening in the news but also in their own company and at home. Many security managers have difficulties establishing a security culture within the company. Mass media is a welcome assistance that supports their efforts. In the best case, the combination of those two, awareness campaigns and media presence, establishes secure behavior as "part of habit" of most citizens in the long run. Since media coverage of security incidents is hardly present in China, citizens, and therefore employees, are not sensitized by this additional communication channel.

The media market is one of the few business areas that is still tightly controlled in China. Foreign firms and individuals are not allowed to control media companies operating in China, regardless of the medium. Therefore, media cannot criticize and control the administration. Privacy breaches by the state are not present in the news.[161] The government therefore freely employs surveillance techniques and builds backdoors that might be exploited by attackers. Furthermore, the media does not exert any pressure on legislation towards information security related laws. As far as my interview results can illuminate this topic, legal pressure on corporate management to care about information security is not existent. The fear of image loss is less present in China because public media does not report security incidents. Especially state-owned companies are hardly ever criticized in the news. Due to this ignorance of all security-related topics, not only legislators and managers but also most individuals undervalue the importance of information security. Employees are not sensitized for security threats and therefore create and ignore security holes that people living in other countries, in which the press often warns about security threats, would be aware of.

---

[161] Even if they would be, the government would probably not be in serious trouble due to Chinese cultural characteristics. Privacy is valued less than in other countries. The power of the government is seldom questioned.

4.6 Concluding Remarks

In this chapter, I presented the insights I gained about security risks and factors influencing information security on an environmental level. Those insights are based on the interviews in conducted in China in late 2006 and a profound and ongoing literature review. I do not present all environmental factors that play a role in outsourcing relationships but only those that my interviewees were most concerned about. All statements do not reflect opinions of single individuals but were mentioned by different people. Furthermore, they can be cross-checked by news articles, books and research papers on Chinese culture or information security and other scientific as well as corporate studies.

I omitted all results that were only relevant for single companies. This thesis is not meant to study particular companies but provides an overview of China as an outsourcing location, primarily focusing on information security issues. In this context, cultural aspects also play a major role. However, they can be seen as part of the *individual level* (in contrast to the environmental and the organizational one). The distinction between those levels is not always clear. Organizational risks that can be seen as dominant in most parts of China and are therefore generic were presented in this chapter. Others that are rooted in cultural characteristics are included later in this thesis. Factors which belong to the organizational level but are not related to the environment or the individual (particularly cultural characteristics) are completely omitted.

The focus of this thesis is to support outsourcing decisions of companies by analyzing the Chinese environment and cultural aspects. Environmental factors could be presented in this chapter without any problem. They can be understood without much background knowledge. They are generic and can be verified by looking at risk management frameworks, press coverage and other studies. Environmental factors are plausible and one can directly engross one's thoughts on every aspect presented. In contrast to environmental factors, this is not possible for aspects on the individual level. Up to now, we were not able to analyze the level of the individual and the impact of culture on informations security because we lack the necessary fundament. Cultural studies can build this solid fundament. Cultural models are necessary for understanding and clustering research results on the individual/group level. Without this knowledge, the results would be single unrelated insights that could not be generalized and could not be transferred to other outsourcing locations.

The following part, which represents the main part of my work, is therefore divided into two chapters. In the first chapter, I introduce cultural models and the status quo of research on the edge between human factors and information security. In the second one, I present my insights on the impact of culture on information security – taking outsourcing of IT services in China as an example.

Part III

Cultural Security Issues in China

Conclusion

The Chinese Outsourcing Environment

Cultural Security Issues in China

Foundations

environment

organization

individual / group

personality

culture

human nature

5

Cultural Foundations

The human factor plays a major role for information security. However, information security managers and risk managers do not have any tools for analyzing it. This chapter provides an introduction to the discipline of cultural studies. Thereby, we will learn about basic concepts and methods that can be used for understanding and judging human behavior. This chapter builds the sound fundament in cultural studies that we need for analyzing the impact of culture on information security.

5.1 The Human Factor in Information Security

Even though many companies have not realized it yet, the human factor has an immense impact on information security. In contrast to the general assumption, a large share of security breaches is carried out by insiders. Even if the attacker is an outsider, social engineering, the art of manipulating people, is becoming a more and more common way of attacking information systems.[1] Social engineering can hardly be prevented by means of technical or organizational countermeasures. Nevertheless, sensitizing and educating employees has been a low priority for many security managers for years. The Global Security Survey by Deloitte shows that this deficiency is slowly resolving.[2] In 2005, most of the survey's respondents were worried about employee misconduct involving information systems but security training and awareness spending

---

[1] See, for example, Committee on Governmental Affairs (2000) and Mitnick and Simon (2002). Robert B. Cialdini, professor of psychology at Arizona State University, wrote two influential books on persuasion, compliance, and negotiation (Cialdini, 2001, 2007). The ideas he describes in his books can directly be applied for attacking a corporate security setting by means of social engineering.

[2] The Global Security Survey is an annual survey comparing the security efforts of organizations worldwide, mainly focusing on financial institutions.

decreased.[3] This trend has reversed. *Security training and awareness* was one of the top five initiatives in 2007, only slightly trailing *access and identity management* and *security regulatory compliance*. In almost all major regions (EMEA, Japan, Canada, USA), the share of organizations whose employees have received at least one training and awareness session on security and privacy in the last 12 months has increased dramatically. Figure 5.1 shows the development over the last couple of years.[4]

Fig. 5.1. Organizations with at least one training and awareness session on security and privacy in the last 12 months

The only region where trainings and awareness programs have decreased is the APAC region (excluding Japan). Deloitte's 2007 study states that *"[o]rganizations in the APAC region are only just beginning to move beyond their heavy reliance on network firewalls, intrusion detection systems (IDS), and patch management systems"*.[5] A large number of Asian companies believe that technological measures are sufficient or that their technological and organizational measures are so weak that fixing them has to be their first priority. Especially in Chinese firms, managers state that technical measures

---

[3] See Deloitte (2005, p. 32)

[4] Please note that for 2005, Japan is included in the APAC region. The chart is based on Deloitte (2005, 2006, 2007). I do not fully trust their exact numbers but Deloitte's studies can be used for observing general trends.

[5] Please note that this data portraits the situation at large financial institutions. Many small and medium enterprises proclaim that they do not have the resources for security trainings.

need to be improved. Organizational measures are regarded as less important. Security trainings and awareness programs are often non-existent. A problem for all companies worldwide is that a *Return on Security Investment (ROSI)* is hard to measure. This is particularly difficult for organizational security measures (in contrast to technology). Therefore, convincing the upper level management to approve IT security spending on security education, extensive background screening of new hires and other organizational security measures is a difficult task. However, as we saw above, the recognition of the human factor has increased.

In research, the upward trend in information security, from technical measures over management activities to institutions, has already been discussed for a couple of years. Basie von Solms describes this trend as three waves.[6] Following a purely technical approach, solving security issues mostly by means of technology (implemented by technical experts), is what he calls the first wave. The second wave broadened the scope of security and created a demand for information security *managers*. In von Solms' words, the third institutional wave further includes the need to build an *information security culture* into the company. *"Senior management realized that the human side of using IT systems, by employees, clients and customers, can cause serious risks [. . .]"*[7] Deloitte's most recent study underlines this statement.

Bruce Schneier explains the same finding, the high importance of the human factor in information security, in his book *Secrets and Lies* with the following words:[8]

> If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Information security managers face difficulties integrating human aspects into their security concepts. Many companies generally do not think long-term oriented. A good comparison are governments. Governments often do not integrate *sustainability* as a core concept into their politics. Politicians are afraid of loosing the next election when they propose new laws that are beneficial to society in the long run but demand sacrifices from each individual in the near future. Managers respectively try to cut spending on information security[9] in order to increase the overall profit of the firm and therefore their own annual bonus. Legal regulations that make managers personally responsible for taking care of operational risks try to countervail those dilemmas. Unfortunately, most Asian countries have not established any of those regulations yet. Without a straightforward model that proves a return on security investment,

---

[6] See von Solms (2000)

[7] See von Solms (2006)

[8] See Schneier (2004, p. xxii)

[9] Especially those programs are often cut which are hard to measure. If the security budget is not cut, it is (in most cases) at least not increased.

especially for spending on organizational measures, managers are unlikely to approve higher budgets for IT security efforts. The above mentioned is even more relevant in countries like China where cost pressure dominates the market.

The importance of legal regulations and business needs has been recognized over the past decade and many security managers have composed security concepts beyond purely technical solutions. However, the human factor has often been disregarded. It is still largely unknown how human behavior influences security within a company. Even security trainings and awareness programs can only be successful if the human factor is properly understood. Introducing those projects without a solid foundation is likely to be a waste of money. Companies, but also researchers, have just started to broaden their horizons. Up to now, they have not looked into social sciences for further insights. Therefore, security solutions look similar all over the world. They to do reflect differences in behavior that can be explained by concepts from psychology and cultural studies. This resistance in corporate management to base security strategies on *soft factors*, derived from humanities, is probably due to the fact that a return on investment in these areas is hard to calculate. Another reason is the lack of studies in this field. Without empirical research proving a direct link between psychology, sociology and cultural studies on one hand, and information security on the other, companies are unlikely to invest in respective security measures. Managers would not even know where to start.

Due to new challenges – outsourcing and cooperation, decentralization of work (e.g. teleworking), etc. – and because of a slow maturation of security research, researchers and practitioners are starting to enter social sciences, striving to gain new insights. Information security research and practice are at a turning point. After purely technological solutions, information security has been seen as a management task. Moreover, security professionals have tried to institutionalize information security. Recently, researchers and practitioners have realized that the weakest link in a security setting is often the human being. Bruce Schneier, for example, writes about the weakest link problem of information security in his book *Beyond Fear*: *"A chain is no stronger than the weakest link. [...] Whatever you do to any other link of the chain won't make it stronger."*[10] Humans often turn out to be this weakest link. This means that any improvements on the technical side do not result in advancements in information security as long as the weakest link – the human being – can still be attacked by an intruder. Schneier proposes three strategies for taking care of the weakest link: *Defense in depth*, *Compartmentalization* and *Choke points.* His ideas can be summarized as: Don't rely on a single countermeasure. Segment your system so that intruders cannot compromise the entire system as soon as they found a single vulnerability. Reduce possible entry points

---

[10] See Schneier (2006, p. 103)

to better understand and supervise those few. These observations unveil two major reasons for focusing on human behavior as a potential security risk:

- As long as the human being persists to be the weakest ling in security settings, any further improvement of technological or organizational measures is useless.
- When employees are aware of security threats, they can add another security barrier. Security turns into a strongest link issue when employees start recognizing anomalies and stop attackers even when they manage to successfully penetrate a technical security measure.

For analyzing human behavior and its impact on information security at least three seemingly separate (but in reality highly interlinked) paths can be followed:[11] *Economics*, *Psychology* and *Sociology/Cultural Studies.*

I do not focus on the field of economics and its impact on information security in this thesis. For more information, please refer to the work by professor Ross Anderson[12] and to the proceedings of the *Workshop on the Economics of Information Security (WEIS).*[13] At *D.A.CH. Security 2008*, Frank Pallas and I presented our thoughts on current security paradigms and how information security should evolve following economic principles.[14] The focus of this thesis rather lies on research in the field of social interaction – cultural studies in particular. I believe that research on the edge between psychology and information security has laid the ground for security research in social sciences. It has broadened the acceptance of the impact of human behavior on security systems. Therefore, a few words about the status quo of the application of psychological insights in the field of information security seem appropriate. First studies that have linked the field of psychology with security (or rather safety in this case) appeared in the field of traffic safety.[15] One theory that has been widely accepted is called *risk compensation*. It attests that individuals, animals as well as humans, adjust their behavior according the the level of risk they perceive. The riskier a situation appears to an individual, the more careful it is in order to reduce the risk to a level that it deems acceptable. On the contrary, if a safety measure is employed and the perceived risk is decreased, the individual behaves less cautiously. The most prominent studies on risk compensation focus on change in behavior regarding the use of seat

---

[11] See, for example, Shostack and Stewart (2008)

[12] See, for example, Anderson (1994a,b, 2001, 2002); Anderson and Moore (2006, 2007a,b); Anderson et al. (2007); Anderson (2008) and Anderson, Böhme, Clayton, and Moore (2008)

[13] In section A.1.1, I already mentioned the Workshop on the Economics of Information Security and wrote about the importance of exploratory research for entering new research fields.

[14] See Glaser and Pallas (2008) Frank is pursuing his Ph.D. in this particular field.

[15] Please note that there is a difference between safety and security. Nevertheless, in this case, there are some interesting similarities that should be discussed.

belts.[16] There are also studies on the use of bicycle helmets,[17] or measures even unrelated to traffic safety, like condoms.[18] While all these studies focus on safety instead of security, the risk compensation theory can easily be transferred to the field of information security. A perceived improvement of security, for example by means of installing a virus scanner on a workstation, might lead the user into the perception that he or she does not need to worry about malicious websites or dangerous e-mail content anymore. The employment of a virus scanner could widen the gap between perceived and actual risk. As a result, the level of security might even decrease by introducing technical solutions without educating the users. Recently, first scientific studies appeared that support the use of concept from social sciences in the field of information security. As for the field of traffic safety, those studies mainly focus on the discipline of psychology. Highly renowned practitioners and researchers like Bruce Schneier[19] and Ross Anderson[20] have started to recognize the need for interdisciplinary research and began working on the relation between psychology and information security. Their most recent effort for bringing together researchers from information security, psychology, economics, anthropology, etc. is the launch of the first *Interdisciplinary Workshop on Security and Human Behaviour (SHB 2008)*. By organizing this highly interdisciplinary symposium, they acknowledge that many other disciplines besides economics and psychology can provide valuable insights into information security research. However, when reviewing the agenda of the SHB 2008, the influence of culture does not seem to be on the radar of the organizers yet. It seems likely that the link between culture and information security will be examined in the near future and that it will be discussed at future workshops on security and human behavior. Plunging into cultural studies raises a variety of complex and highly significant questions. Those need to be addressed in the future.

How important is the integration of organizational measures – focusing on the human factor and not only on technical solutions – into our security strategy if we outsource our IT anyway? Is it possible to create an information security culture for the entire company? What additional hurdles do multinational and therefore multicultural companies face? Can we force our outsourcing provider to use our codified security policies? Do security awareness campaigns need to be based on different national or ethnical values, or even religious beliefs? What kind of role do our own and our outsourcing provider's corporate culture play? Do people from other countries understand our security policies the same way we do? How do cultural characteristics influence human behavior in a way that raises or lowers security risks? Only

---

[16] See, for example, Adams (1982, 1995) or Harvey and Durbin (1986)

[17] See, for example, Janssen (1994) or Adams and Hillman (2001)

[18] See Richens, Imrie, and Copas (2000)

[19] See Schneier (2008)

[20] See Anderson and Moore (2007b)

cross-cultural research, conducted from an information security point of view, can answer those questions.

5.2 The Infancy of Cross-cultural Research in Information Security Research

Analyzing the impact of culture on other disciplines is a new phenomenon. This can be seen as one of the main reasons why there has not been much research on the influence of culture on information security. Especially in business science, researchers were hoping to find 'culture-free' models. They were looking for concepts and theories that allowed them to predict economic outcomes and behavior within firms worldwide.[21] Many researchers believed for a long time that business and economic models can be transferred to other countries and societies without alteration. They assumed that models which worked in one country could successfully be employed by companies in other countries.

Even today, many business books written by US-American 'management gurus' are translated and shipped all over the world. They are seen as best practices without questioning whether the proposed business practices are based on cultural assumptions that might not be valid in other countries.[22] A one-size-fits-all approach, assuming that American management practices can successfully be transferred to Asian companies or subsidiaries, can lead to interpersonal misunderstandings and disputes. Karen L. Newman and Stanley D. Nollen found that team performance is higher when management practices are congruent with the national culture of the team members.[23] This raises complex questions because many companies and project teams already are or are turning multinational, with teams composed of people with dozens of nationalities and different social backgrounds.

Differences in management style were first acknowledged when Japanese management practices proved highly successful and Western companies started adopting Japanese methods. Today, terms and practices like *Kaizen*[24] and *5-S*, or rather the entire field of *lean manufacturing*, are an integral part of many Western firms. However, they have their roots in Japanese culture and were adapted by Western companies after observing the success of Japanese enterprises. Another expression of Japanese culture is the Japanese *Keiretsu*. A keiretsu is a federation of companies with business relationships but also mutual shareholdings, either vertically or horizontally integrated.[25] Most keiretsu were formed after World War II as a reinvention of *Zaibatsu*, formerly dominant conglomerates broken up by the Allies. Both concepts, keiretsu and

---

[21] See Kutschker and Schmid (2006, p. 663)
[22] See Kutschker and Schmid (2006, p. 665)
[23] See Newman and Nollen (1996)
[24] See Imai (1986)
[25] See Miyashita and Russell (1995)

zaibatsu, are not focused on profit-maximization but rather reflect the importance of relationships in Japanese society (similar to the concept of Guanxi in China). They underline the cultural value of long-term orientation by minimizing the opportunity for hostile takeovers.[26]

The rise of culture in management science did not start with national cultures. It rather started with the concept of corporate cultures.[27,28] Considering the fact that researchers were hoping to find culture-free models that are transferable across borders, this development was a logical consequence. Forming a corporate culture that is consistent in the entire firm worldwide is an intriguing vision. However, practice showed that subsidiaries have to adapt to local conditions. A uniform corporate culture is therefore impossible.[29]

The way management science has integrated the concept of culture also influenced the relation between culture and information security. The focus of management science only recently shifted from corporate cultures to the impact of national cultures on business practices. This explains the reluctance of information security researchers and practitioners to examine national cultures. As we will see in the next section (5.3), research has been conducted on *security culture* (corporate culture with a focus on information security). The impact of regional cultures on information security is still unknown. Therefore, security policies, awareness campaigns, etc. are developed in the headquarter and afterwards transferred to foreign subsidiaries and suppliers. This reminds us of the mistakes companies made before, transferring management practices to other countries without regional adaption.

In the following, I explain the difference between *information security culture*, as a security measure, and the role that *regional cultures* play in information security.

---

[26] Some foreign enterprises followed the keiretsu approach and tried to build similarly strong relationships with their suppliers. One prominent example of a foreign company trying to adapt the Japanese keiretsu concept is the strategy change that took place at Chrysler Corporation in the end of the 1980s. See Dyer (1997)

[27] See Kutschker and Schmid (2006, p. 663 ff.)

[28] For an in-depth description of different scopes of culture, see section 5.4.2.

[29] Many foreign enterprises operating in China have started to withdraw their expatriates, replacing them with local professionals. Those new managers are often educated abroad but still deeply rooted in the Chinese culture. Foreign managers have not only realized that the management in China needs to speak the local language but also that it has to understand the local culture in order to get a sense for the feelings and needs of the employees. Furthermore, management practices have to be adapted to local conditions. The regional culture plays a major role.

5.3 Security Culture versus the Impact of Culture on Security

In recent years, information security professionals and researchers started realizing the importance of the human factor. They began the journey to understand human behavior in order to manage security risks. It is important to underline that this is a two-step process. First, human behavior has to be understood so that it can be managed (or rather guided) afterwards.

In the second phase of this process, managers use different tools. While technical solutions and formal rules were the most prominent security regulators for decades, a third regulator, *social norms* (informal rules), is starting to gain recognition. Those informal rules can be seen as part of a *security culture*. A security culture tells employees what kind of behavior is desirable and which behavior is inappropriate. As for any kind of culture, at the core of security cultures are values and norms. If the security of the company is established as a core value of its corporate culture, employees behave in a secure manner because they regard this as desirable. On the other hand, if they behave differently, in a way that threatens the firm, they object the social norms of the company's culture. If they violate those informal rules (norms), they are punished by their colleagues on a social level. No hierarchical sanctions are necessary. A security culture is defined, implemented and adjusted by security managers in order to steer the behavior of their employees.[30] Security cultures can be seen a tool to guide human behavior. Managers try to use it as a third regulator, besides technology and formal rules, to reach a high level of information security. Security cultures are implemented in a corporation for this specific purpose. They unify the understanding of security within the firm, educate employees and motivate them to behave in a secure manner. The scope of a security culture is the corporation itself. Beyond the borders of the organization, the security culture looses its purpose. Security cultures can therefore be seen as subculture of corporate cultures.[31]

All three regulators, including informal rules (or security cultures), can be seen as a way of guiding human behavior. However, in order to be able to guide human behavior, it is necessary to understand why people behave in certain ways. What is happening right now is that researchers and practitioners try to make the second step (managing human behavior) before the first one (understanding how humans behave). Psychology plays a prominent role in understanding individual behavior. Cultural studies can explain behavior based on similarities within groups. In order to be able to manage human behavior, one needs to understand underlying principles. Understanding the behavior of employees and to predict specific security threats based on human

---

[30] Organizations can already exhibit a security culture without the interaction of management. However, the problem that is most often discussed is how to create security cultures. Security cultures can be regarded as planned. They are build by managers to increase the level of security.

[31] See Schlienger and Teufel (2002)

behavior fundamentally different from the concept of security cultures. In order to understand the behavior of employees and its impact on information security, one needs to dramatically enlarge the scope of the concept of culture. Not only corporate cultures influence the behavior of employees but also their individual cultural backgrounds. As I will explain in depth in section 5.4.2, individuals always belong to different cultural groups, based on their age, gender, education, nationality, etc. The primary goal of this thesis is to shed light on the influence of regional cultures on information security. This thesis supports the first step of the process presented above, understanding behavior based on cultural characteristics. Security culture, as a regulator that helps guiding behavior and thus managing security within a firm, is a very different concept, a tool that can be used in the second phase of the process.

It is crucial to point out this fundamental difference between *information security culture* and *the impact of culture on information security*. While a security culture is a security measure that managers can use for controlling human behavior, analyzing the impact of culture on information security is necessary for understanding the impact of human behavior. Implementing a security culture without a proper understanding of the behavior of employees is making the second step before the first. In contrast to the influence of culture on security, the importance of security cultures has already been analyzed by a few researchers and practitioners. In the following, I give a brief overview of research on information security cultures before coming back to the main theme of this thesis, the impact of culture on information security.

5.3.1 Excursus: Research on Information Security Culture

Thomas Schlienger and Stephanie Teufel, from the University of Fribourg, are two of the few researchers who bring together concepts developed by cultural scientists with information security research. In *Information Security Culture: The socio-cultural dimension in information security management*, they present Edgar H. Schein's three layer model of culture.[32] According to Schein, culture is composed of *(1) artifacts and creations, (2) collective values, norms and knowledge* and *(3) basic assumptions and beliefs*. Schlienger and Teufel use those three levels to explain the concept of *security culture* and how a security culture can be implemented within a corporation.[33,34] Even though they should be acknowledged for their interdisciplinary research, they also make the second step before the first. They try to provide managers with a tool to regulate the behavior of their employees without a proper understanding of human behavior. Schlienger and Teufel guide security managers

---

[32] See, for example, Schein (1999)

[33] See Schlienger and Teufel (2002)

[34] For further research on information security culture by Schlienger and Teufel, see Schlienger and Teufel (2003a,b) and Schlienger and Teufel (2005) (in Sasaki, Qing, Okamoto, and Yoshiura (2005)).

by broadening their horizons and showing them that security cultures are a new tool for raising the level of security. They challenge the status quo of solely relying on technology and formal rules. Thereby, they make important progress in adapting to the challenges of decentralized organizations. However, they do not contribute to a better understanding of the influence of culture on information security.

Kuusisto, Nyberg and Virtanen follow Schlienger and Teufel but enlarge the scope by including the intercultural dimension. However, their focus also lies on pursuing a unified security culture. In *Unite Security Culture*,[35] they scrutinize the question whether it is possible to create a company-wide security culture even in multicultural settings.[36] They make five assumptions that need to be taken into account for creating a unified security culture. The most important one clarifies the necessity of common values for creating a unified security culture:

> 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.[37]

Kuusisto, Nyberg and Virtanen understand that security cultures are not a static tool that can be transferred to other countries without adaption. Since common values do not exist across different nationalities, it is difficult to create a mutual understanding of information security in a multinational company. Even harder is creating this same understanding in two different firms from value-wise divergent nations. Unfortunately, Kuusisto, Nyberg and Virtanen also talk about security culture as a tool instead of analyzing the impact of culture on information security.

There are a few other researchers besides Schlienger, Teufel, Kuusisto, Nyberg and Virtanen who recognize the need for research on the edge between information security and cultural studies. Even the OECD recognized the need to create a 'culture of security' and made it the main principle behind their publication *OECD Guidelines for the Security of Information Systems and Networks*.[38] However, I miss researchers making the first step (understanding human behavior) before the second one (managing it). Scientific research needs to be conducted on values of different social groups, different (regional) cultures, and their impact on information security. Afterwards, research on security culture as a management tool can continue with a more solid foundation.

---

[35] See Kuusisto, Nyberg, and Virtanen (2004)
[36] See also Helokunnas and Kuusisto (2003)
[37] See Kuusisto et al. (2004)
[38] See OECD (2002)

5.4 Introduction to Culture

In their 2002 paper *Toward a theory-based measurement of culture*, Straub et al. state that *"cross-cultural information systems research, in general, remains in a state of infancy"*.[39],[40] They mention two reasons for the lack of research in this interdisciplinary field: The absence of a unified definition for the term *culture* and that people not necessarily only belong to one culture. In order to build a sound foundation for analyzing the impact of culture on information security, the term culture needs to be defined and different perspectives introduced. An appropriate definition not only demands the creation of a mutual understanding of the term culture but also setting a scope that is appropriate for analyzing the actual research question. This thesis shows that many security threats can be explained based on cultural characteristics. The first step towards understanding how culture affects information security is to define the term culture and to briefly discuss prominent concepts.

According to the cultural theorist Raymond Williams, who examined the etymology of culture, the term *"emerged in the sixteenth century in English (and other European languages) as a process that denoted the tending or rearing of crops and animals"*.[41] Fons Trompenaars further says that *"it comes from the same root as the verb 'to cultivate', meaning to till the soil: the way people act upon nature"*.[42] This already depicts a couple of important aspects of culture. Culture is learned over a long period of time. It manifests itself in the interaction with nature, or more broadly, in the interaction with one's environment. Since interaction with our environment is part of our daily life, our culture is deeply rooted in ourselves. We act according to it in an unconscious manner. Those aspects correspond to a great extent with contemporary definitions of culture.

One of the earliest definitions of culture is coined by Sir Edward Burnett Tylor. In 1871, he wrote that *"[culture is] that complex whole which includes knowledge, belief, art, morals, law, language and any other capabilities and habits acquired by man as a member of society"*.[43] This definition again highlights aspects I just presented as culture's etymological foundation. We will see in the following that also Tylor's definition is very close to today's understanding of culture. Tylor's definition was used by anthropologists, the main group of researchers focusing on culture in the late 19th century, for about 50 years.[44] When the concept became more commonly used in other research areas, numerous definitions of culture were developed by researchers

---

[39] See Straub, Loch, Evaristo, Karahanna, and Srite (2002)

[40] Information security research is a subfield of information systems research. The infancy is even more apparent at the intersection of information security and cultural studies.

[41] See Williams (1976) as in Clegg, Kornberger, and Pitsis (2005, p. 287)

[42] See Trompenaars and Hampden-Turner (1997, p. 23)

[43] See Tylor (1871)

[44] See Edmonds (2002, p. 182)

and practitioners from various different disciplines. In 1952, the American anthropologists Alfred Kroeber and Clyde Kluckhohn compiled distinct definitions of culture and published them in their compendium *Culture: A Critical Review of Concepts and Definitions.*[45]

The *United Nations Educational, Scientific and Cultural Organization (UNESCO)* defines culture as follows:[46]

> [. . .] culture should be regarded as the set of distinctive spiritual, material, intellectual and emotional features of society or a social group, and that it encompasses, in addition to art and literature, lifestyles, ways of living together, value systems, traditions and beliefs, [. . .]

The UNESCO uses the terms *society* and *social group* as central to its definition of culture. As numerous as the definitions of culture are the different interpretations of those two terms. They are defined differently, depending on the discipline that researchers come from. Prominent definitions come from the disciplines psychology, economy and history — just to name a few. Turner for example defines a social group as *"two or more individuals who share a common social identification of themselves or, which is nearly the same thing, perceive themselves to be members of the same social category"*.[47] These common social identification can be manifold. We can distinguish according to various different criteria, e.g. nationality or region, religion, native language, gender or workplace. The concepts of culture and society (or social group) are highly interlinked. One cannot exists without the other. People share cultural characteristics with a social group they spend a lot of time with: their colleagues. Many companies have a corporate culture which defines how people should interact.

A Dutch researcher and probably the most prominent figure in the field of cultural studies, Geert Hofstede, took another view on culture and its impact at the workplace. He analyzed the affect of national culture on values that influence people's behavior at work.[48] He describes three levels of uniqueness of *mental programming* that define how we think and act. Those three levels are *human nature*, *culture* and *personality*.[49]

Human nature is a unifying element that is inherited within one's genes and therefore the similar for all humans unrelated to their social background. Human nature is the *"operating system that determines one's physical and basic psychological functioning"*.[50] There are major differences in the functioning of many animals and humans, but for humans, the basic physical and psychological structure is the same. This thesis is about behavioral differences

---

[45] See Kluckhohn and Kroeber (1952)
[46] See UNESCO (2002)
[47] See Turner (1982, p. 15)
[48] His model is increasingly used in management-related disciplines, but also in social sciences. See Baskerville (2003, p. 3 f.)
[49] See figure 5.2 as in Hofstede and Hofstede (2005, p. 4)
[50] See Hofstede and Hofstede (2005, p. 4)

Fig. 5.2. Three Levels of Uniqueness in Mental Programming by Hofstede

that that can be linked to security threats. Human nature is therefore out of scope of this thesis.[51] *Personality*, at the top of the triangle, is specific to each individual. According to Hofstede, it is partly based on one's individual set of genes and partly influenced by *"collective programming (culture) as well as by unique personal experiences"*.[52] There certainly is an impact of personality on information security. However, because it is specific to each individual, it is impracticable to analyze underlying patterns and to compare the behavior of people with different backgrounds, which is necessary to point out general tendencies. *Culture* is the level of mental programming I mainly focus on. It is learned and therefore specific to the social environment. In contrast to personality, it is not based on unique individual but on general experiences that are similar for a whole group of individuals. It is therefore the intermediary level, not as universal as human nature and not as specific as personality, formed and displayed in the interaction of people.

Without other individuals, culture would not exist. If a person grew up alone, without any interaction with other individuals, his experiences would be specific to himself and not shared with anyone. Therefore, there would not be any layer of culture that he shares with others as part of his mental

---

[51] Culture is often described as a major reason why humans differ from animals and managed to specialize in various functions. Peter J. Richerson and Robert Boyd argue that *"the human cultural system arose as an adaption because it can evolve fancy adaptations to changing environments rather more swiftly than is possible by genes alone. Culture would never have evolved unless it could do things that genes can't!"* (Richerson and Boyd, 2006, p. 7) Edward T. Hall draws similar conclusions based on research by Weston La Barre. He argues that man accelerated the evolutionary process by shifting his evolution from his body to his extensions – extensions being technological innovations but also elements like language and writing. (Hall, 1990a, p. 3 f.) The nature of evolution, which was formerly believed to be solely based on genes, has therefore been altered in fundamental ways by a level of mental programming that Hofstede calls culture.

[52] See Hofstede and Hofstede (2005, p. 5)

programming. His thinking would only be based on what Hofstede calls human nature and personality.[53] In case this person grew up in a social group, he would share experiences and concepts with the others.[54] There would be a unifying culture that can be observed by observing different individuals within the group. If one individual leaves the others, external observers might not be able to tell whether certain aspects of his mental programming are culture-based or part of his personality.[55] In the absence of other individuals, culture does not reveal itself.

Culture, shared between the members of a social group, manifests itself in various ways. Hofstede points out four different levels, which he believes cover the entire concept. Those levels are values, rituals, heroes and symbols. He organizes those levels in an onion model. Values are the core of the onion, symbols its outermost layer. Hofstede distinguishes between the core *(values)* and the outer layers, which Hofstede grouped as *practices.*[56],[57]

The closer the layer to the inside of the onion, the deeper it is rooted into a person's mental programming (culture). If a layer lies on the inside, it is hard or might even be impossible to change. Furthermore, inner layers are more hidden from outside observers than outer layers. The outmost layer, *"[symbols,] are words, gestures, pictures, or objects that carry a particular meaning only recognized by those who share the culture."*[58] Language, flags or status symbols are common and easily observable examples of symbols. New symbols can be acquired and old ones abandoned rather easily. Symbols are therefore presented as the outmost, most superficial, layer of culture. *"Heroes are persons, alive or dead, real or imaginary, who possess characteristics that are highly prized in a culture and thus serve as models for behavior."*[59] One can argue that heroes are not an own layer of culture but rather an expression of values, hidden within the cultural onion. However, this can be argued for all practices. Heroes and other practices, especially traditional ones, can also be seen as role models that deliver and reinforce social values for new generations. *"Rituals are collective activities, technically superfluous to reaching desired ends, but which within a culture are considered as socially essential. They are therefore carried out for their own sake."*[60] Ways of greeting, the

---

[53] Those are the bottom and top lay of mental programming. See 5.2

[54] The aspects that are shared between individuals are described more specific in the following. Experiences and concepts should therefore be regarded as a placeholder until I introduce concepts like values and practices.

[55] Obviously, some behavioral patterns can only be formed by interacting with others. Nevertheless, they can only be described as part of a culture if they are shared by more than one person.

[56] See figure 5.3 as in Hofstede and Hofstede (2005, p. 7)

[57] Fons Trompenaars developed an own onion model, very similar to Hofstede's. See page 126

[58] See Hofstede and Hofstede (2005, p. 7)

[59] See Hofstede and Hofstede (2005, p. 7)

[60] See Hofstede and Hofstede (2005, p. 7)

Fig. 5.3. Hofstede's Onion of Culture

organization of meetings or ceremonies, etc. are excellent examples of rituals. They often do not fulfill an obvious purpose but are rooted deep into a culture and might express underlying values in a similar way as heroes do. In the core of Hofstede's onion are values. *"Values are broad tendencies to prefer certain states of affairs over others."*[61] They determine what individuals describe as good or evil, beautiful or ugly, dangerous or safe, normal or abnormal, etc. Since most *"values are acquired early in our lives"*[62], they are manifested very deep into our mental programming and hard to change.[63] Moreover, they are rarely visible to outsiders and often only observable through practices.

Fons Trompenaars, a scholar of Hofstede and a cross-cultural researcher himself, splits the core of culture – what Hofstede calls values – into two dimensions. He calls those individual dimensions *norms* and *values*. *"Norms are the mutual sense a group has of what is right or wrong. Norms can develop on a formal level as written laws, and on an informal level as social control. Values, on the other hand, determine the definition of good and bad, and are therefore closely related to the ideals shared by a group."*[64,65] Fons Trompenaars and Charles Hampden-Turner vividly describe norms as *the way we should behave*

---

[61] See Hofstede and Hofstede (2005, p. 8)

[62] See Hofstede and Hofstede (2005, p. 8)

[63] As opposed to practices which can be changed more easily and also later in life.

[64] See Trompenaars and Hampden-Turner (1997, p. 22)

[65] For a deeper analysis of norms and its function as a regulator, see section 5.4.1.

and values as *how we aspire or desire to behave.*[66] They further provide an example of how norms and values show in reality. If Japanese are asked why they bow, some people say that they would like to greet others, show respect to elder or to those with a higher social status. This behavior is based on values. Others say that they do it because other people around them do the same thing. In that case, they are led by a social norm. Values are deeply rooted into ourselves, into our own personal mental programming. Norms can also be posed on us by others.[67] Hofstede describes norms as *"standards for behavior that exist within a group or category of people. In case of the desirable, the norm is absolute, pertaining what is ethically right. In case of the desired, the norm is statistical: it indicates the choices made by the majority."*[68] Norms therefore rather act as an institution and should be positioned on a more superficial layer.[69] A divergence of values and norms might lead to tension in a society.[70] This often happens in multicultural settings and when a person enters a new cultural environment. This individual takes his own value system with him and is subject to conflicting formal rules or informal social norms. This tension can only be resolved if both sides are aware of the fact that they might possess different, or even conflicting, value systems. Accepting cultural differences without labeling the other person's cultural background as inferior is crucial.

Besides the difference to Hofstede concerning social norms, Trompenaars also developed an own onion model for culture.[71] He goes one step deeper than Hofstede. Under the layer of norms and value (as in the desirable and the desired), he puts a new core which he calls *basic assumptions.* Trompenaars believes that basic assumptions are even deeper rooted than values. They are hardly ever questioned. People just behave according to those basic assumptions naturally without thinking about them. An example of basic assumptions would be human equality, which is rarely questioned in most Western societies. According to Trompenaars, one can distinguish basic assumptions from norms and values by asking questions about them. If the other person is irritated or confused, like many Westerners would be when asked

---

[66] See Trompenaars and Hampden-Turner (1997, p. 22)

[67] This might explain why Hofstede decided to stick to the concept of values as most central to our mental programming. Hofstede also makes a distinction but does not call the results norms and values. For Hofstede, values manifest in two ways: *the desirable* and *the desired.* (Hofstede, 1984, p. 21) Values determine the desired to a large extent. The desirable can be influenced by others in form of institutions – e.g. social norms. See section 5.4.1

[68] See Hofstede and Hofstede (2005, p. 21)

[69] Helen Spencer-Oatey's decided to follow this approach. She developed an own onion model, which I will introduce shortly.

[70] The same is true for a gap between values and other institutions like formal regulations.

[71] See figure 5.4

about the reason for human equality, the inquirer knows that he discovered a basic assumption.

Fig. 5.4. Trompenaars' Cultural Onion

However, it is hard to draw a line between values and basic assumptions. Similar to basic assumptions, values are followed in daily life unconsciously. Values and basic assumptions are both mostly invisible to outside observers. Most people would not only be irritated when their basic assumptions are questioned but would feel the same way if their values are scrutinized.

Helen Spencer-Oatey mixes the onion models by Hofstede and Trompenaars and Hampden-Turner and develops an own cultural onion which solves many problems discovered above.[72]

She puts basic assumptions and values on the same layer, at the core of the onion. They are often visible to others on the next layer, which she newly introduces and calls *beliefs, attitudes and conventions*. This layer is similar to the core. It can be described as its practical manifestation. Beliefs, attitudes and conventions influence the next layer, *systems and institutions*. Norms are standards for behavior that exist within a group.[73] They can therefore be seen as institutions, part of the third layer. Spencer-Oatey's outmost layer is

---

[72] See figure 5.5 as in Spencer-Oatey (2000, p. 5)

[73] See section 5.4.1 for further information on norms, part of culture, as a fundamental institution.

Fig. 5.5. Spencer-Oatey's Cultural Onion

split into two sections. It consists of elements that manifested themselves in behavioral patterns, *rituals and behavior*, and non-behavioral items like *artifacts and products*. If we reduce the item she calls behavior to only those behavioral patterns that are culture-based and not part of an individual's personality, Spencer-Oatey's model provides the most holistic and most precise model. It allows to combine blurry elements like basic assumptions (or key beliefs) and values into a single layer, an improvement over Trompenaars' model. Furthermore, it allows a clear definition of norms by putting them on an institutional layer. Neither Trompenaars nor Hofstede mentioned this layer explicitly.

In the following section (5.4.1), I elaborate on social norms as a regulator, a standard for desirable behavior shared within a group. I further explain how social norms, as part of culture, set a frame for the constitution of other institutions.

5.4.1 Culture as a Fundamental Institution

As explained earlier, social norms are an integral part of a culture. By taking a brief look at *institutional economics* we can understand their pivotal role in society and compare social norms to other institutions.

Richter and Furubotn define institutions as *"the grin without the cat"*[74] or *"the rules of the game without the players"*.[75] Those rules consist of formal regulations, informal norms and their enforcement characteristics.[76,77] Laws and other formal regulations as well as social norms (as an integral part of each culture) can therefore be regarded as institutions. The main difference between those institutions lies in their acceptance by society and their role as a framework for other institutions. Institutions can be divided into two clusters – *fundamental* and *secondary institutions*. Social norms, money, human rights and language are often categorized as *fundamental institutions*. They build a frame that all other institutions need to adhere to. They predefine external boundaries. This hierarchical order is visualized in figure 5.6.[78] This order can also lead to conflicts between the institutions and thereby conflicts within society.

An example of how this theoretical observation explains day-to-day problems is described in section 4.3. Law can be seen as a secondary institution that is based on fundamental ones.[79] It must adhere to the rules that social norms set. If it does not follow these rules and operates outside of the frame of what is acceptable to social norms, the law is disobeyed by the people whose behavior it should regulate. The same also applies to any other kind of formal regulation. Information security policies are such formal regulations. According to the rules of institutional economics, they must be based on fundamental institutions in order to be followed. This implies that security policies are not independent of the cultural setting in which they are used and that they cannot be transfered from one country to another without a proper adaption to new cultural characteristics.

Social norms, and thereby culture, are a fundamental institution. They are deeply rooted in society. Without obeying the rules that those fundamental institutions entail, secondary institutions are bound to fail.

5.4.2 Different Scopes of Culture

The term culture is often used without deliberately defining its respective scope. However, the scope significantly changes the meaning of the term culture. Whereas culture always is about learned characteristics similar to all

---

[74] They refer to *Alice's Adventures in Wonderland* by Lewis Carroll: *"[. . .] this time [the cat] vanished quite slowly, beginning with the end of the tail, and ending with the grin, which remained some time after the rest of it had gone. 'Well, I've often seen a cat without a grin,' thought Alice; 'but a grin without a cat! It's the most curious thing I ever saw in my whole life!'"* See Carroll (2000, p. 66)

[75] See Furubotn and Richter (2005, p. 9)

[76] See North (2005, p. 22)

[77] See also Ostrom (2005, p. 824 f.)

[78] The institutional hierarchy is based on Dietl (1993, p. 74). See also Picot et al. (2005, p. 11) and Wernick (2007, p. 77 f.)

[79] See Picot et al. (2005, p. 9 ff.)

```
┌─────────────────────────────────────────────────────────┐
│                 Fundamental Institutions                 │
└─────────────────────────────────────────────────────────┘
                     build a framework for
        ┌─────────────────────────────────────────┐
   ───▶ │   Secondary (deduced) Institutions       │ ◀───
        │              level 1                      │
        └─────────────────────────────────────────┘
                     build a framework for
        ┌─────────────────────────────────────────┐
   ───▶ │   Secondary (deduced) Institutions       │ ◀───
        │              level 2                      │
        └─────────────────────────────────────────┘
                     build a framework for
        ┌─────────────────────────────────────────┐
   ───▶ │   Secondary (deduced) Institutions       │ ◀───
        │              level n                      │
        └─────────────────────────────────────────┘
```

Fig. 5.6. Institutional Hierarchy

members of a group, the composition of the group changes the impact of culture on research and practice. The reason for analyzing corporate cultures usually differs from research on gender, generational cultures or regional cultures to a great extent. Just having mentioned a few scopes of culture, I will deepen on this matter in the following. As shown in figure 5.7, the ways of defining culture can be manifold.

Common scopes are set by clustering people who live in the same region or work in similar industries or professions.[80] For other research questions, the gender or the ethnicity, which seem to be rather atomic scopes, might be the appropriate unifying element. There is an unlimited number of possible scopes. The kind of cluster chosen always depends on the specific question.

Some scopes can be clustered and the number of people within these scopes can be enlarged by increasing their size. However, enlarging the scope can blur the image because it often reduces the number of commonalities possessed by people within this group. Creating clusters by examining the culture of

---

[80] Even within the same country and the same profession there are cultural differences. These are often due to different corporate cultures. Mjøs (2004) shows those differences by analyzing cultural characteristics of the employees of three Norwegian airline companies.

Fig. 5.7. Different Scopes of Culture

people living in a certain neighborhood, researchers are likely to find many similarities, especially if the individuals grew up in this area. The number of people within this scope can be increased by enlarging the area (taking the city or the country as the respective scope). This can reveal new cultural similarities, but on a more superficial level. The smaller the scope, the more likely that the people within this scope share the same values and practices – the same culture.

Taking the region or the workplace as the unifying element are two possible ways of creating flexible clusters. But also most of the other potential scopes, shown as single entities in figure 5.7, can be subdivided into various smaller scopes. Taking age as an example, the scope could be people who are born in the same century. The scope can be scaled down by only observing people who belong to the same generation, are born within the same year or even on the same day. The latter ones are less likely to show unique commonalities that are not shared by others born within a slightly larger time frame. On the other hand, defining the scope too large might not be useful for observing similarities and deriving scientific results either. If one would take all people who are born after and before Christ as two different groups, one might find unifying elements for each of the groups. There would certainly be some characteristics that are influenced by religion. However, those might not be the characteristics one is looking for. Talking about religion, this is another example of a scope that is often regarded as a single entity but can be subdivided into different clusters. Judaism, Christianity and Islam all belong to the same root. They are all abrahamic religions. They therefore exhibit similarities so that the

entire group of people who belong to abrahamic religions can be culturally differentiated from Hindus and Buddhists.[81]

As it becomes obvious, when talking about different cultures, it is important to clearly define the scope. As discussed before, setting the scope too small or too large can both lead to inappropriate results. However, there is no general rule for how to set the scope. Defining it as the country in which people live might be appropriate for one research question, others might require a smaller region like the city as the cultural scope. Conducting research on cultural matters, it is often advisable not to cluster by one field but to combine many of them. This acknowledges the fact that one person not only belongs to a single cultural group but is likely to be a member of many different ones. Analyzing the cultural similarities of Turkish women who are in their twenties, live in Berlin and hold a university degree might make sense for a specific research question.

One should also take into account that our world is gradually turning into a multicultural melting pot. A few centuries or even decades ago, traveling was much more time consuming and less affordable so that cultures did not mix as much as they do today. This melting of cultures can also lead to a loss of one's cultural identity. This can be observed in communities of people from a specific country living together in another country. Growing up in different (maybe even opposed) value systems can lead to substantial inner conflicts. In those settings it is more difficult to judge what is right or wrong, just or unjust. Immigrants also suffer the problem to define their own origin and identity. Europe is another example of this identity crisis. In Europe, people with increasingly different backgrounds merge. Without unambiguous and well-communicated unifying values, many Europeans face the problem of grasping their own identity.

This multiculturality obviously does not only lead to problems of finding one's own identity but also to intercultural clashes in business. Those clashes pose serious difficulties on security management and research. Firms cannot be regarded as German, US-American or Chinese anymore but are a melting pot of people with a multitude of cultural origins. Corporate governance in general, and information security management in particular, needs to pay attention to emerging intercultural conflicts.

5.4.3 Scope Chosen for this Thesis

In the course of this thesis, I examine security risks that companies face while outsourcing IT services in and to China. I therefore decided to set a regional scope. To be more precise, I focus on the culture and the behavior of Mainland Chinese. China's national culture is the main object of investigation but I also compare it to other national cultures.

---

[81] Even specific abrahamic religions like Christianity can be subdivided further into Catholics, Protestants, etc.

In research and practice, it is common to refer to *the Chinese* or *the Chinese culture*. However, China is an extremely complex and versatile country. In different parts of China, one certainly makes different experiences, is taught different views, etc. It seems appropriate, even necessary, to exclude the two Special Administrative Regions (Hong Kong and Macao) and Taiwan from this analysis.[82] When talking about Chinese and Chinese culture in the following, I refer to Mainland Chinese.

As noted above, I fully acknowledge that individuals are members of various cultural groups and that by restricting myself to the analysis of one particular cultural group, I take a specific perspective that influences the results of my research. Furthermore, this decision does not imply that all individuals belonging to the cultural group chosen (in this case all Mainland Chinese, or for comparison, all US-Americans, all Indians, etc.) are homogeneous. Their cultures certainly vary and they exhibit cultural characteristics besides the particular group that is observed.[83] Nevertheless, a certain perspective needs to be chosen in order to focus and to create a scope of discussion. It would be infeasible to analyze cultural issues from all possible perspectives. Since the goal is to provide researchers and practitioners with insights into security risks resulting from cultural characteristics and intercultural differences while outsourcing in China (Mainland China in this case), a comparison of the regional Mainland Chinese culture with national cultures of other countries is most appropriate.

Please note that the results of my thesis are not necessarily limited to national cultures. The security issues discussed are based on characteristics that can be evaluated for other cultural scopes in the same way. The results are transferable to other countries and different settings. However, the cultural characteristics dominant in Mainland China are the main focus of this work.

5.5 Established Cultural Models

For analyzing the impact of different national cultures on information security, we need a sound foundation of well-established cultural models. In order to

---

[82] I fully acknowledge that there are many regional cultural differences within Mainland China as well. Xinjiang, Tibet, but also parts of Inner Mongolia, Liaoning, Ningxia, Guangxi, etc. could be named as special regions because of their high percentage of non-Han inhabitants. Guangdong can be considered to be a special case because of its role as the home of the Cantonese language and its proximity to Hong Kong. Cultural characteristics of people living in the rich East (coastal areas) vary greatly from those inhabiting the rural West. Likewise, various other cultural differences can be found. However, these differences are neglected in this thesis. The regional cultural scope of this thesis is Mainland China.

[83] There many special cases like Chinese nationals who were raised in other countries and there are many foreigners who are permanent residents in China. For other special cases, primarily focusing on cultural differences within Mainland China, see previous footnote.

build such a solid fundament for my research, I present the work of many renowned intercultural researchers in the following. I especially focus on those who built cultural models and classifications that can be applied to national cultures. I use their models and their research results as a foundation for my own work.

5.5.1 Introduction to Cultural Models

The first question that should be raised is: *What is a cultural model?*

Ruth Benedict, author of two groundbreaking books in the field of cultural studies[84] and one of the most influential American anthropologists, writes about her own profession: *"He [the anthropologist] is interested in human behaviour [...] He is interested in the great gamut of custom that is found in various cultures, and his object is to understand the way in which these cultures change and differentiate, the different forms through which they express themselves, and the manner in which the customs of any peoples function in the lives of the individuals who compose them."*[85]

Cultural models mainly deal with the aspect of how different cultures differentiate. They explain variations in behavior based on a specific set of characteristics. This set should be exhaustive and cover most variations in behavior. The main goal of cultural models is to answer three basic questions that Alex Inkeles and Daniel J. Levinson call *standard analytic issues*: *relation to authority*, *self-conception* and *primary conflicts and the ways of dealing with them*.[86] There are two major approaches of how to analyze these questions by examining cultural characteristics: *Typological models* and *Dimensional models*

Typological Models

Typological models focus on ideal types that are easy to imagine. Most typologies are easy to observe because they describe *"a small number of traits that are readily observable from a distance"*.[87] This becomes clear when we look at common typologies. The most common typology, coming from the field of anthropology, is the division according to race. Other typologies like the division into *masculine and feminine*, *hetero- and homosexual*, *different age or income groups*, etc. are also often used. In the second half of the twentieth century, the distinction between *capitalist* and *communist* or *First World*, *Second World* and *Third World* became very common. Coming back to cultural studies and the application of typologies in cultural studies, certain characteristics are often attributed to people of a particular nationality. Germans

---

[84] See Benedict (1989, 2005)
[85] See Benedict (1989, p. 1)
[86] See, for example, Inkeles and Levinson (1997, p. 43 ff.) or Chan (1999, p. 100)
[87] This quote is by a researcher with a background in biology. See O'Neil (2008)

are very punctual, US Americans superficial, Asians very group oriented, etc. In a sense, typologies are like stereotypes. They generalize real characteristics and reduce complexity. They are therefore easy to grasp and to communicate. On the other hand, they tend to oversimplify. It is difficult to compare countries based on typologies because they only allow the distinction between black and white, right and wrong. Typologies cannot describe nuances and the magnitude of a particular characteristic.

Dimensional Models

Dimensional models, on the other hand, were developed for the very reason of comparing cultural characteristics in different cultural settings. As Geert Hofstede states in his book *Cultures and Organizations – Software of the Mind*: *"A dimension is an aspect of a culture that can be measured relative to other cultures."*[88] Dimensions do not represent a single phenomena but group together various characteristics that occur in combination. Whereas typologies often describe a particular aspect of a cultural setting (e.g. Germans are accurate), dimensions describe general characteristics on a higher level of abstraction. For each country, a score is normally assigned to each characteristic. Cultural dimensions are therefore rooted in empirical data. Their scales are often normalized. The country with the strongest support for a certain characteristic is defined as 100 or 10 (or any other number, depending on the precision of the scale and decision of the researcher), the one with the lowest support is set to 0. Gaps between the scores of different countries describe cultural differences that might turn into intercultural conflicts. Cultural researchers try to limit the number of dimensions. More than 10 different dimensions are uncommon for a dimensional model. However, the dimensions should still exhaustively describe differences between countries. Besides comparing different countries, dimensional models can also be used for monitoring cultural changes that take place in a particular country over time. Because cultural dimensions describe cultural characteristics on an abstract level and are presented as values on a scale (which need to be interpreted), they are harder to explain than typologies.

Both models, typological and dimensional, can of course only describe tendencies of cultural settings. An individual German can exhibit a cultural characteristic that does not fit to the typological or dimensional model at all. Those variations cannot be described by cultural models. They rather describe the overall attitude, behavior, etc. that is dominant in a society.

Summing up, the difference between typological and dimensional models can be explained in computer science terms. Typological models and dimensional models are like *digital and analog*. Whereas typological models only allow a few states (like binary, either true or false), dimensional models describe characteristics on a scale that allows a seemingly continuous range of

---

[88] See Hofstede and Hofstede (2005, p. 23)

states. Each model has its advantages, depending on the intention of the researcher. If one wants to compare different cultures or the development of cultures over time, dimensional models are more appropriate. For presenting and explaining cultural characteristics of countries, typological models are useful due to their simplicity. Typological models and dimensional models are therefore often used at the same time. Based on data from dimensional models, countries are clustered and certain typologies are assigned to the entire group of countries. Those hybrid models are very common and used by many researchers. Even though I occasionally use typologies during this thesis, this thesis is primarily based on dimensional models and their empirical data.

In the course of this section, I introduce many cultural researchers and their cultural models. The focus of their work either lies on intercultural communication (leading to intercultural conflicts) or on cultural values that determine the behavior of members of a cultural group. Out of those researchers I present, Edward T. Hall is the one with the strongest focus on communication. All others mostly analyze cultural values of different cultural settings. The concept of values has already been described in detail in section 5.4. It will become a lot clearer when we review the cultural concepts of Kluckhohn and Strodtbeck, Hofstede, Trompenaars, etc.

Up to now, I have written very little about the second branch of intercultural research – intercultural communication. In the next section, I explain the basic concepts of intercultural communication. With this knowledge, it becomes easier to fully grasp Edward T. Hall's model and communication-related security threats.

5.5.2 Intercultural Communication

As I just mentioned, there are two major branches of intercultural research: Cultural models based on *Value Systems*[89] and *Intercultural Communication*.

Culture-based security threats can have two different origins. They can be based on the *behavior of a single individual* or on *intercultural clashed between two or more people* (e.g. employees of an outsourcing provider and its client). Whereas a lot has been and will be said about value systems, we still need to provide a sound fundament for analyzing the second branch – intercultural communication.

The first step is to define the term *intercultural communication*. Richard E. Porter and Larry A. Samovar say: *"Intercultural communication occurs whenever a message produced in one culture must be processed in another*

---

[89] It is important to keep in mind that value-orientation is a highly important and practical method for understanding culture. However, it covers only part of what we defined as culture. (Parsons and Shils, 1951b, p. 159) A lot of research has been done on what Hofstede calls cultural practices. Value systems are more important for this thesis than practices because values change slowly. Furthermore, they can be quantified in order to compare different countries.

culture."[90] A lot of problems that occur in intercultural communication also take place in day-to-day communication between people with the same cultural background. Whenever two or more people interact, they base their interpretation of the other person's word on own assumptions. This leads to miscommunication. We need to understand what happens when people interact, why it happens, the effects it has, and what we can do to influence the outcome of this interaction.[91] In order to understand many problems of intercultural communication, we should take a look at the very basics of communication theory.

Shannon–Weaver Model of Communication

The most fundamental model of communication was developed by one of the most influential computer scientists – Claude Elwood Shannon.[92] He published his ideas 1948 in an article called *A Mathematical Theory of Communication*[93] which later started off an entire research field – information theory.[94] His ideas became widely known after he published them in a book which he co-authored with Warren Weaver in 1963.

The Shannon-Weaver model describes the basics of the communication process.[95] It defines seven essential elements of communication: *Information Source*, *Transmitter*, *Channel*, *Noise*, *Receiver*, *Destination* and the *Message* itself. Those elements form a communication model which is shown in figure 5.8.

The *information source* is a person, a group or an IT system that wants to send an information to a specific *destination* (again, a person, a group or an IT system). Since the *message* can be a human being or an IT system, it is an abstract concept with various real world representations. In order to transmit information, the information source uses a *transmitter* (a telephone, computer, pen and paper, one's own voice, etc.) which transforms the message

---

[90] See Porter and Samovar (1994, p. 7), in Samovar and Porter (1994)

[91] See Porter and Samovar (1994, p. 7)

[92] In information security, Shannon is famous for his quote *"the enemy knows the system"* (Shannon's maxim) which is a reformulation of *Kerckhoffs' principle*. See Shannon (1949, p. 662). Kerckhoffs said that every cryptosystem must be secure even if the attacker knows everything about the system except the key. See Kerckhoffs (1883a,b). Kerckhoffs and Shannon both criticize an approach called *security by obscurity*. This approach relies on the secrecy of vulnerabilities. Security is achieved by hiding vulnerabilities instead of fixing them. Both researchers say that the system must still be secure if the attackers knows everything about the system (except the crypto key). This principle is today widely accepted not only for cryptosystems but for any kind of security setting.

[93] See Shannon (1948), also published as Shannon (2001)

[94] See, for example, Pierce (1980)

[95] Hollnagel and Woods refer to the Shannon-Weaver model as *"the mother of all models"*. See Hollnagel and Woods (2005, p. 11)

Fig. 5.8. Shannon–Weaver Model of Communication

into a representation that can be sent through a communication channel. The *receiver* collects the message and again transforms it into a representation that is understood by the destination. This communication process does not always work properly because the message can be decoded in another way than is was encoded. Communication problems occur if the message lacks context and if the transmission was disrupted because of noise (background noise, many people speaking at the same time, interfering signals, water corroding handwritten letters, etc.).

In order to adapt this communication model to human interaction, it is sometimes simplified for a more natural use in interpersonal communication. Afterwards, it only consists of three elements: *Sender*, *Message* and *Receiver*. Some representations also cover the entire Shannon-Weaver model. Therefore, two more steps – encoding and decoding of the message (which can be verbal or nonverbal) – are added again. The new model (see figure 5.9) is equivalent to the first representation of the Shannon-Weaver model.

Fig. 5.9. Model of Interpersonal Communication

The main deficiency of the transmission model is that the sender is the decision maker, the active entity in a communication, and the receiver is purely passive. In reality, communication is always a two-way process in which sender and receiver continuously change roles (or rather take both roles at the same time). The receiver continuously responds to the sender. Speaking slightly philosophically and in the words of Paul Watzlawick, *"One Cannot Not Communicate"*.[96] Another deficiency of the transmission model is that the interpretation process is oversimplified. The receiver does not simply absorb the information from the message but interprets it in his own cultural context.

Norbert Wiener, the 'father of cybernetics',[97] addressed the first insufficiency of the model – the lack of communication back from the receiver to the sender. He published two highly influential books around the same time as Shannon was working on his paper.[98] Wiener proposed and formalized a communication principle that he called *feedback*. In his words, *"[feedback is] the property of being able to adjust future conduct by past performance"*.[99] He says there are two kinds of feedback, positive and negative. Without feedback we would not be able to know if our communication partner understood our message (acoustically but also contentwise). Feedback is therefore an essential element of communication. It motivates us to resend messages, sometimes also in a rephrased manner, if we think the receiver has not understood them in the way they were meant. An adapted communication model, in which I incorporated feedback, is presented as figure 5.10.

Since feedback is a message itself, it is also encoded and decoded and can be misinterpreted by the receiver (the original sender). Exactly the same problems that occur with the message can be observed for feedback. Understanding feedback is only said to be easier because feedback does not transport as much content as the message itself and thereby does not open that much room for misunderstandings. Even if the feedback only represents agreement or disagreement, it can be misunderstood. Whereas nodding the head up and down usually means agreement ('yes') in most parts of the world, in parts of Greece, Turkey, Bulgaria, and a few other countries, this gesture stand for the

---

[96] I will address a more axioms by Paul Watzlawick later in this section.

[97] The interdisciplinary research field *cybernetics* focuses on the analysis of communication and control mechanisms (including the feedback principle) in complex systems. Researchers from the fields of sociology, game theory, system theory, psychology, mathematics, etc. all made important contributions to cybernetics. The entire research field was started with the *Macy Conferences*, focusing on *Feedback Mechanisms and Circular Causal Systems in Biological and Social Systems.*

[98] In 1948, Wiener wrote *Cybernetics: Or the Control and Communication in the Animal and the Machine.* Two years later, he published *The Human Use of Human Beings.* See Wiener (1961) and Wiener (1988)

[99] See Wiener (1988, p. 33)

Fig. 5.10. Communication Model with Feedback

exact opposite (disagreement, 'no'). Shaking the head from left to right can mean 'yes', for example in Saudi Arabia, Malaysia and also Bulgaria.[100]

But even after incorporating feedback to the model, it still lacks some important elements that are responsible for problems in intercultural communication. *Context* (time, place, content of earlier discussions, etc.) and the *relationship between sender and receiver* are two important examples. We should keep in mind that these aspects exist and that they are responsible for the outcome of communication.

Schulz von Thun's Communication Quadrant

The analysis of communication based on the Shannon-Weaver model already disclosed many problems that can occur during communication. In order to deepen this analysis and to show that communication – even between communication partners with similar cultural backgrounds – can easily lead to misunderstandings, I briefly describe *Schulz von Thun's Communication Quadrant.*

Friedemann Schulz von Thun, a German psychologist, says that the exact same message can be interpreted in four different ways.[101] His communication quadrant consists of four levels (or sides): *content*, *relationship*, *demand* and *self-revelation.* The receiver can simply decide to only interpret the content of a message (its facts) or he can analyze what the message says about his relationship to the sender. The demand side reveals the intention of the sender and the self-revelation side shows what the sender discloses about himself (intentional or unintentional).[102]

---

[100] See Holstein and Gubrium (2001, p. 341), Holstein and Gubrium (2003, p. 435), Payr and Trappl (2004, p. 112) and Mitchell (2000, p. 89)

[101] Schulz von Thun published his ideas in various books. The most relevant ones concerning his communication quadrant, are Schulz von Thun (1981, 1989) and Schulz von Thun, Ruppel, and Stratmann (2000).

[102] By adding the last two dimensions, Schulz von Thun enlarges Watzlawick's ideas. Watzlawick focuses on two sides of communication – *content* and *relationships.* His axioms of communication are introduced later in this section.

I do not want to discuss this model in detail. I would like to present an example that shows how important context is for deciphering a message. Without the necessary context, messages can be interpreted in any of these four ways and thereby misunderstood. In the following, I present all four possible interpretations of the sentence: *I am cold.*[103]

- *Content:* It is cold in here/today. (just stating the fact)
- *Relationship:* I am cold. You should know that I'm suffering. Why don't you feel with me.
- *Demand:* It is cold in here. Could someone please shut the window?
- *Self-Revelation:* I am suffering because of the cold.

All four interpretations have totally different meanings. Sender and receiver are both surprised or even upset if the other interprets the message in another way. If the sender is annoyed because there are many people sitting next to the window but nobody closes it, even though it is extremely cold in the room (demand side), and the receivers interpret the message on the content side (answering: 'Yes, that's true. It is colder today than normally in July. Isn't it beautiful that we are not sweating in office for once?') and thereby do not see any reason to act, trouble in inevitable. Matters get worse when the relationship side is involved.

Schulz von Thun's communication quadrant shows that communication is always ambiguous and can be interpreted in various ways. Context is highly important and if a situation (or a message) lacks context, it is likely to be misinterpreted. People from different cultural settings have different assumptions. Their experiences induce a particular interpretation of a message. Having different backgrounds – maybe even different mother tongues – words have different nuances for communication partners. Sayings and idioms might not exist in other languages and language is used differently in general. Disrespecting context is one of the main mistakes in communication.

Paul Watzlawick's Axioms of Communication

I would like to end this introduction to intercultural communication with five axioms of communication by Paul Watzlawick. Watzlawick was an Austrian communication theoretician, sociologist, psychotherapist and author of various books. In 1967, he published a book on styles and structure of interpersonal communication together with Janet Bavelas and Don Jackson: *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes.*[104] In this work, Watzlawick composes a list of five axioms that are crucial for communicating effectively. The focus of these

---

[103] Please not that the expression *I am cold* is ambiguous and can mean *it is cold in here/today* or *I'm a cold person* (emotionally). We will focus on the first interpretation.

[104] See Watzlawick, Bavelas, and Jackson (1967)

axioms does not lie on intercultural issues. However, as mentioned earlier, most problems that occur in communication in general are multiplied when people with divergent backgrounds interact. Watzlawick's five axioms summarize many insights we already gained in this section but also provide some new aspects that we should keep in mind. His axioms help us to analyze information security threats that are based on problems of intercultural communication. In the following, I briefly address all axioms consecutively.[105]

1. *One cannot not communicate.*
   The first one is Watzlawick's best-known axiom of communication. It says that any form of behavior is communication. If two people pass each other in office without saying a word, they communicate with each other.[106] Everybody knows the situation of sitting in a doctor's waiting room. In the waiting room, most people try hard to communicate that they are not interested in talking. This is perfectly understood by the others, even though nobody says a word. There is also a typical Chinese behavior that often leads to intercultural misunderstandings. Many Chinese do not reply to messages, or phone calls, if those messages include a request that they cannot satisfy. If a Chinese had to say 'no', he or she might *loose face.* Saying 'no' would at least have an impact on the interpersonal relationship. In order to guard against those problems, it is common not to reply at all. By showing this behavior a Chinese is not not communicating. His lack of action is a way of communicating with the inquirer. His way of communicating is everything else but rude, as it might be interpreted by an interculturally inexperienced Westerner. The interpretation of a message always depends on the context, and the cultural context is highly important. That all being said, there is one restriction to this axiom. In detail, it can be stated as: *"[I]t is impossible for members of a communication system not to communicate. If they are not communicating, they have not formed interdependencies, and thus their group of two or more people is not a communication system."*[107] This means, if two people pass by each other on the street, have no relationship whatsoever, do not notice and maybe not even see each other, they might actually not communicate. Thus, it is important to understand that one cannot not communicate purposefully. One cannot decide not to communicate and thereafter restrain from doing it.

2. *Every communication has a content and relationship aspect.*
   The second axiom is the predecessor of Schulz von Thun's communication

---

[105] For good introductions to Watzlawick's five axioms, see, for example, Picot, Reichwald, and Wigand (2008) or Dainton and Zelley (2004).

[106] For example: I do not want to talk to you. Please leave me alone. I am afraid of talking to people I don't know. I am busy. etc. The interpretation of communication always depends on the context.

[107] See Whaley and Samter (2007, p. 317)

quadrant. Watzlawick and his colleagues say that there are always two sides to a message – the content of the message and a manifestation of the relationship of the two (or more) communication partners.[108] The relationship aspect is often misinterpreted because it is implicitly coded into the message. It can be expressed verbally but is normally part of nonverbal communication. The relationship aspect makes a big difference. It can allow the distinction between a discreet request or a command. It can make the communication partners feel that they are on equal footing and that their relationship is based on mutual respect or that one person is trying to exert dominance over the other.[109] Especially in Asian cultures, the relationship aspect of communication plays a highly important role. If it is disregarded, misunderstandings and cultural clashes are bound to happen.

3. *The relationship of the communication partners is established by the use of punctuation during encounters.*
Using punctuation marks in written communication means breaking texts (or sentences) into small units. A comma in written language stands for a small pause in spoken language.[110] Where this pause is made does influence communication but is not the meaning of this axiom. Punctuation here rather means the way communication partners split their communication into different pieces – on a more abstract level. Communication is normally a stream of interactions without a real beginning and an end. However, we do split our interactions with others into various sequences. A call starts with picking up the phone and ends with hanging it up again. But the conversation that we have over the phone might have started earlier and might not end with us putting the phone down. It might end weeks or even years later. On the other hand, what we consider a single conversation (e.g. a talk that we have face-to-face) can be broken into different sequences (for example the moment a quarrel started). Different streams of conversation might be interlocked but persist over longer periods. *"Certain behaviors are perceived as a response to other ones."*[111] Without punctuation, we can not make sense of our conversations. Without using punctuation in a similar manner, two communication partners are bound to misunderstand each other because they see statements in different contexts. *"[...] divergences in punctuation can occur easily, particularly in intercultural communication, which often lead to considerable misunderstandings and even the failure of the communication process as*

---

[108] This is a major difference to Schulz von Thun's model. Whereas his communication quadrant says that a message *might be interpreted* in four different ways, Watzlawick says that *there are always* both aspects coded into the message – content and relationship.

[109] See Dainton and Zelley (2004, p. 56)

[110] See Van Oorschot and Hogerhuis (2006, p. 99)

[111] See Littlejohn (2003, p. 236)

a whole."[112]

4. *Human communication makes use of digital and analog modes of communication.*
   "Analogic codes are those in which the symbol actually resembles the object it represents. [...] Digital communication is that in which the symbol and the meaning of the symbol are arbitrarily linked."[113] Nonverbal messages are often analog, verbal communication tends to be digital. Crying is an analog for sadness. Gestures and mimics often show analogies to the emotion they are related to. Therefore, analogs are largely similar in different cultures. Verbal communication is digital because words can hardly represent the real meaning they stand for. *"[T]here is nothing inherently catlike about the word cat, nor is there anything particularly democratic about the word democracy."*[114] The meaning of words is culturally determined. Words are symbols without any natural relation to their meaning. However, there are exceptions for both modes. There is nonverbal communication that is not analog (e.g. the OK sign - building a circle with thumb and index finger) and verbal communication might not be digital but analog because it resembles the real world (e.g. the words 'click', 'hiccup', 'bang', etc.). Since analogs are a direct representation of objects, they are likely to be understood across different cultures. Digital communication is normally impossible without proper knowledge of the language (acquired by years of learning). Nevertheless, there are examples of analogs which are misleading. Holding up two fingers (either the thumb and the index finger or the index finger and the middle finger) means two in most Western cultures. With two hands, Westerners can count up to ten. Chinese can be seen as more effective. They can show all numbers up to ten using only one hand. Raising the thumb and the index finger – which means two in Western cultures – means eight in China. This reason for this Chinese interpretation is that the fingers resembles the Chinese character 'ba' which means eight. It is said that many Westerners already made this mistake in a Chinese bar and ordered eight beers instead of two. An understanding of the communication partner's culture and its symbols is therefore indispensable.

5. *Communication is based on symmetrical and complementary relationships.*
   A relationship is symmetrical when there are no differences in hierarchy between communication partners and when they perceive each other as peers on the same level. Complementary relationships, on the other hand, exist when communication partners behave as if they were on different levels. For example, if *"Mike is sarcastic to you, [and] you are sarcastic to*

---

[112] See Picot et al. (2008, p. 80)
[113] See Dainton and Zelley (2004, p. 57)
[114] See Dainton and Zelley (2004, p. 57)

Mike" you have a symmetrical relationship. It is complementary if *"Mike is sarcastic, [and] you whine".*[115] It does not matter if there is a real difference in hierarchy. It does not need to be rooted in corporate or social hierarchy. All that matters is whether people behave in a complementary manner. In intercultural communication, complementary relationships are very common because people often feel inferior (or superior) to communication partners from other countries. But also within many cultures with a strong power distance,[116] complementary relationships are typical.

Paul Watzlawick's axioms do not build a complete communication model. Nevertheless, they offer valuable insights into interpersonal communication. Furthermore, they can be applied to communication between two or more firms. If we keep in mind axiom number one – *One cannot not communicate* – and analyze communication between outsourcing providers and their clients, we will notice many problems of intercultural communication.

But now we should leave theoretical considerations behind and directly plunge into an introduction of the most important cultural models and their inventors.

5.5.3 Clyde Kluckhohn, Florence Kluckhohn and Fred Strodtbeck

The couple Clyde and Florence Kluckhohn, both American anthropologists, developed one of the first ethnographic models that compares communities based on cultural values.[117] They explain their focus by stating that the *"emphasis on values grows out of an anthropological tradition of culture assessment".*[118] In later years, especially after Clyde Kluckhohn's death in 1960, Florence Kluckhohn intensively worked together with Fred Strodtbeck.

Clyde Kluckhohn's interest in intercultural issues started early in his life. It was intensified when he had to live in a Navajo Indian community in order to improve his health. He learned their language and customs and published various books about their culture.[119] He presents his ideas on the concept

---

[115] See Dainton and Zelley (2004, p. 57 ff.)

[116] See section 5.5.5

[117] Clyde Kluckhohn defines the term *value* as *"[...] a conception, explicit or implicit, distinctive of an individual or characteristic of a group, of the desirable which influences the selection from available modes, means, and ends of action."* See Kluckhohn (1951, p. 395 ff.)

[118] See Kluckhohn and Strodtbeck (1961) as cited in House, Javidan, Hanges, and Dorfman (2002, p. 5) and House, Hanges, Javidan, Dorfman, and Gupta (2004, p. 16)

[119] See *To the Foot of the Rainbow* (Kluckhohn, 1927), *Beyond the Rainbow* (Kluckhohn, 1933), *Navaho Classification of Their Song Ceremonials* (Wyman and Kluckhohn, 1938), *An Introduction to Navaho Chant Practice* (Kluckhohn and Wyman, 1940) and *Navaho Witchcraft* (Kluckhohn, 1944)

of culture in two major works: *Mirror for Man: The Relation of Anthropology to Modern Life*[120] and *Personality: In Nature, Society, and Culture*[121] He even makes the distinction between biology (human nature), culture and personality which is later used by Hofstede as the three levels of mental programming.[122]

In 1961, one year after Clyde Kluckhohn's death, his wife Florence and Fred Strodtbeck published their groundbreaking work *Variations in Value Orientatiions*,[123] presenting the *Value Orientation Method*. This value orientation method is used for comparing cultures based on their values. For their publication, Kluckhohn and Strodtbeck analyzed cultural values of five small communities in the Southwest of the United States of America: a Texan homestead community, a Mormon village, a Spanish-American village, a decentralized Navaho Indian Band, and a highly centralized pueblo of Zuni.[124]

By comparing those five communities, they identified five value orientations (or dimensions): *Relationship to Nature*, *Time*, *Character of Human Nature*, *Human Action*, and *Relationships to Others*. The questions they tried to answer are *What is the appropriate relationship to nature?* (relationship to nature: subordinate to nature, harmony with nature, dominant over nature), *How should we best think about time?* (time: past, present, future), *What is the basic nature of people?* (human nature: evil, mixed, good), *What is the best mode of activity?* (human action: being, becoming, doing) and *What is the best form of social organization?* (relationship to others: hierarchical, collateral, individual).[125,126]

I do not want to describe every dimension in detail because my research is based on other dimensions (namely those by Edward T. Hall and Geert Hofstede). However, Kluckhohn and Strodtbeck *"laid the groundwork for [other cultural researchers like] Hall, Hofstede, and Trompenaars and Hampden-Turner"*.[127] Even recent work in the field of cross-cultural research, for exam-

---

[120] See Kluckhohn (1949)

[121] See Kluckhohn and Murray (1948)

[122] See Kluckhohn and Murray (1948, p. 27)

[123] See Kluckhohn and Strodtbeck (1961)

[124] See House et al. (2004, p. 440) or Kluckhohn and Strodtbeck (1961)

[125] These explanations are taken from Gallagher (2001) based on Kohls and Knight (1994)

[126] Kluckhohn and Strodtbeck identified and worked on a sixth dimension, *the conception of space*, which can be seen as private, public or a mixture of these two. (See, for example, Parker (2005, p. 192), Thomas (2001, p. 49) or Day, Zaccaro, and Halpin (2004, p. 305)) However, they did not fully include it in their analysis because they argued it was not thoroughly researched at that time. (See, for example, Earley (1997, p. 158)) The conception of space later became central to Edward T. Hall's model of culture. He devoted an entire book, *The Hidden Dimension*, to the use of space in different cultures and called his concept *the theory of proxemics*. (See Hall (1990a), first published in 1966, and section 5.5.4)

[127] See Kampf (1999, p. 152)

ple the GLOBE Study,[128] is still based on many dimensions that are directly derived from those defined by Kluckhohn and Strodtbeck.

5.5.4 Edward T. Hall

Edward T. Hall, born in 1914, is an American anthropologist, cross-cultural researcher, consultant to the American government and author of various books. Like Clyde Kluckhohn, Hall lived and worked with the Native American Navajo community (but also with Hopi) and thereby made his first intercultural encounters.[129] During World War II, Hall served as a soldier for the US Army in Europe and the Philippines. He experienced and observed how difficult the contact between his fellows and local communities was. With this background, he later worked for the Foreign Service Institute at the Service Department to prepare employees and diplomats for intercultural encounters in the countries they were assigned to. In 1959, Hall published his first major work on intercultural communication – *The Silent Language*[130] – which became the first in a series of books focusing on cultural dimensions.

Hall never developed an own holistic cultural model. He analyzed different dimensions which he identified through his experience in numerous cultural environments. In contrast to many other researchers, Hall's dimensions are not based on one major survey. They are the result of many years of research and his consulting experience.[131] Unlike Hofstede and others, who describe differences and unifying themes of various countries based on cultural values, Hall mainly focuses on communication and human interaction as cultural characteristics. For Hall, *culture* and *communication* are completely interlinked:

> Culture is communication and communication is culture.[132]

He describes culture as a system that knowledge management practitioners would describe as *collective memory*:[133]

> Culture is many things, but it is primarily a system for creating, sending, storing, and processing information.

Hall distinguishes between four dimensions, all related to cultural aspects of communication. These dimensions are *Context Orientation*, *Monochronic versus Polychronic Time*, *Space* and *Preferred Message Speed*.

---

[128] See House et al. (2004)

[129] He reviewed his experiences in Hall (1995).

[130] See Hall (1990b). He also published a shorter version in the Harvard Business Review, which pushed his popularity. See Hall (1960)

[131] See Kutschker and Schmid (2006, p. 703)

[132] See Hall (1990b, p. 186)

[133] The term *collective memory* was coined by Maurice Halbwachs. He describes culture as a memory embedded in societal constructs like families and religions. See Halbwachs and Coser (1992)

Context Orientation

Context orientation determines the amount of information that needs to be exchanged during communication so that the receiver fully understands the message of the sender.[134]

In high-context cultures, only a small portion of the information that is transmitted is explicitly coded into the message itself. People are often inter-linked into a strong web of relations and hierarchies which makes communication besides the actual message possible. In high-context communication, a big share of information lies in contextual elements like the *"physical context or [is] internalized in the person, while very little is in the coded, explicit, transmitted part of the message"*[135]. There is no need to additionally codify this information into the message because communication partners understand each other based on the context.[136] In low-context cultures, the opposite is the case. *"[T]he mass of the information is vested in the explicit code."*[137] Information needs to be codified explicitly, as part of the message, because the lack of contextual information would lead to misunderstandings on the receiver side.

Fig. 5.11. High-Context versus Low-Context Cultures

Since relationships and context are not obvious when entering a new setting, high-context cultures are usually harder to enter because the outsider

---

[134] For further information on the *reception model* and problems in decoding messages, see section 5.5.2 or Hall (1992, p. 128 ff).

[135] See Hall (1989a, p. 91)

[136] See Kutschker and Schmid (2006, p. 703)

[137] See Hall (1989a, p. 91)

lacks context. Therefore, communication can be misunderstood. It can be very confusing for people who do not understand the unwritten rules that exist within the culture. In general, low-context cultures are easier to enter because rules are mostly explicit and communication carries the content of the message explicitly. Members of high-context cultures do not need this explicit form of communication because a large part of the content is revealed through the context. High-context communication is possible because members of high-context cultures tend to have fewer and longer lasting relationships than it is the case in low-context cultures. In the latter ones, relationships rather fulfill a purpose and are established for achieving a certain goal. They can be broken up afterwards more easily. Since relationships play an important role in high-context cultures, communication is often more indirect and makes extensive use of non-verbal elements. It follows a spiral towards the point that needs to be discussed. By this means, the feedback from the receiver can better be analyzed. The relationship is unlikely to be affected because the topic can be changed if the communication partner seems uncomfortable. In contrast, members of low-context cultures try to come straight to the point because they strive for short, efficient forms of communication. The relationship plays a less important role.[138]

Monochronic versus Polychronic Time

"In monochronic cultures, time is experienced and used in a linear way [...] Monochronic time is divided quite naturally into segments; it is scheduled and compartmentalized, making it possible for a person to concentrate on one thing at a time."[139] Polychronic cultures, on the other hand, do not have distinct time slots arranged in a linear order. Time segments blur and different things can happen simultaneously. Mediterranean people, for instance, have a polychronic understanding of time. They can upset people with monochronic backgrounds because those regard time as tangible. Time can be lost or even wasted from a monochronic perspective. This is because monochronic societies regard time as a linear concept. Time is running from the past, to the present into the future. Polychronic people, on the other hand, regard time as circular. Time and actions need to be reflected in front of past and future events. One can always come back to something that has been started earlier.[140] Agreements are not fixed but only represent a description of the status quo.[141]

---

[138] There are many similarities with Trompenaars' dimension of universalism (low-context) and particularism (high-context). Looking at Trompenaars' dimensions, further insights can be gained. See section 5.5.6

[139] See Hall and Hall (1990b, p. 13)

[140] See Hall and Hall (1990a, p. 16 ff.)

[141] For further insights into practical applications of this dimension, I would like to refer to an interesting study conducted by Rose, Evaristo and Straub on *"differences in delay attitudes and perceptions of web-based delay [web download time] in monochronic and polychronic cultures."* See Rose, Evaristo, and Straub (2003)

Fig. 5.12. Monochronic versus Polychronic Time

In polychronic cultures, time does not matter as much as personal relationships. Sticking to deadlines is not important because they are seen in a larger context.[142] If the deadline of a delivery that was previously agreed on is not necessary anymore for the other party, polychronic people do not understand why they should deliver on time. They are *"concerned about delivering in time for you"* because they value the relationship and do not want to get you into trouble.[143]

Space

"It has long been believed that experience is what all men share, that it is always possible somehow to bypass language and culture [...]"[144] This assumption was made because one thought that a brain receives the same input if it is fed with the same data. Edward T. Hall coined a term *proxemics* which describes the man's use of *space* as a concept of culture.[145] He states that people from different countries *"inhabit different sensory worlds"*. Therefore,

---

[142] The relationship is only part of this larger context.

[143] See, for example, Trompenaars and Hampden-Turner (1997, p. 137 ff.). Trompenaars and Hampden-Turner describe are very similar dimension but call it *sequential versus synchronic time.*

[144] See Hall (1990a, p. 2)

[145] See Hall (1974) and various articles by Hall on this topic

they react differently to the same input. Those sensory inputs are not necessarily visual. They can also be auditory, thermal, kinesthetic and olfactory.[146] The concept of space affects various everyday situations. Arabs, for example, maintain a shorter physical distance during conversations than Americans.[147] In American business culture, doors are always open. In Germany, they are closed. American relationships are defined according to space (amongst various other factors). Being neighbors already implies a close relation. Relationships in the United Kingdom rather focus on social status.

Preferred Message Speed

Message Speed is the dimension that Edward T. Hall added most recently. It describes the speed with which information is preferably encoded and decoded in different cultures. Television, for example, is a medium that supports fast and usually more shallow messages. Research journals or other print formats carry deeper messages that need more time to decipher. Hall also regards people and human relationships from a perspective of message speed. *"In essence a person is a slow message; it takes time to get to know someone well."*[148] Regarding a person as a message is an excellent example for describing cultural differences in *preferred message speed*. In the United States, it is easy to get to know people in a superficial way. Europeans and especially people from most Asian countries prefer deeper relationships that need time to develop and grow.

Whereas many other researchers regard their dimensions as distinct (mutually exclusive), Hall states that his dimensions are interlinked. High-context societies, for example, tend to be polychronic and most low-context culture regard time as monochronic. Furthermore, high-context cultures also prefer a slow message speed. It takes time to establish a deep relationship that is necessary for high-context communication. However interlinked Hall's dimensions are, splitting them into different dimensions reveals valuable insights because each dimension looks at cultural characteristics from a unique perspective.

5.5.5 Geert Hofstede

Geert Hofstede is a Dutch researcher, trainer and author who mainly worked on analyzing national and organizational cultures. Hofstede holds a Masters degree in Engineering and a Ph.D. in Social Psychology. In 1965, he joined IBM where he founded and managed the *Personnel Research Department* of IBM Europe. Between 1967 and 1972, he developed a questionnaire and

---

[146] See Hall and Hall (1990b, p. 11)

[147] Arab and American sensory apparatus work differently and their expectations of *personal* and *social distance* therefore diverge.

[148] See Hall and Hall (1990b, p. 5)

evaluated cultural values of IBM employees in more than 70 different countries. His research is regarded as the most influential study of differences in behavior due to different regional cultures. He is the most cited researcher in the field of intercultural management and every recent study still references his work.[149]

At IBM, Hofstede developed a model with four dimensions which he used to differentiate the cultures of the countries that participated in his study. The dimensions he introduced are *Power Distance*, *Individualism*, *Masculinity* and *Uncertainty Avoidance*.[150] Based on those four dimensions 49 percent of empirically found variance can be explained.[151] This shows that his dimensions cover a large part of cultural characteristics but are not exhaustive. Michael Bond, professor of psychology at the Chinese University of Hong Kong, and some of his colleagues conducted a similar study in the 1980s which confirmed most of Hofstede's findings. However, they also revealed a Western bias in Hofstede's work and that due to this bias his four dimensions were not fully exhaustive for East-Asian cultures.[152] On that account, Hofstede added a fifth dimension later on, which he called long-term orientation (LTO). In the following, I introduce all five dimensions of Hofstede's final model.

Power Distance Index (PDI)

> the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally[153]

In every society, there are inequalities in the distribution of power. In countries with a large power distance, power is distributed less equally than in small power distance communities. High power distance means that it is socially accepted and sometimes even socially supported that some members of society have more power than others. Unequal distributions of power is often rooted in the history of a country – as most other cultural values are as well. It can be based on race, religion, etc. The traditional Indian caste system, which attributes certain roles in a society to people within a particular caste, is an excellent example of a system in which power is distributed unequally.[154] The membership in a particular caste does not necessarily say

---

[149] See section 6.1.4

[150] Hofstede's entire work is based on cultural values. He differentiates between the desirable and the desired. Both are expressions of cultural values.

[151] See, for example, Kutschker and Schmid (2006, p. 711) or Berry, Poortinga, Segall, and Dasen (2002, p. 400)

[152] See Chinese Culture Connection (1987)

[153] See Hofstede and Hofstede (2005, p. 46)

[154] In India, the caste system and the social inequalities related to it have greatly been reduced. Even member of the caste which was formerly called *the untouchables* can today receive high-ranking governmental posts. However, in some parts of the country, the system is still prevalent.

anything about power or financial status but there were and still are strong tendencies towards power distribution. The caste system can therefore be seen as a system of hierarchy. At the work place or at school, people from countries with a large power distance show respect to their subordinates (managers, teachers, parents, etc.). They are obedient and sometimes even expect to be told what to do. Hierarchy, not only in society but also in organizations, is prevalent and centralization is popular. On the contrary, in countries with a small power distance, teachers and managers treat their students and subordinates as equals. They expect their participation and initiative to come up with new ideas and to manage their assignments independently. Decisions are reached in a democratic process and a decentralization of organizations and thereby a decentralization of power is common.

Individualism (IDV)

> pertains to societies in which the ties between individuals are loose: everyone is expected to look after himself and his or her immediate family. Collectivism as its opposite pertains to societies in which people from birth onward are integrated into strong, cohesive in-groups, which throughout people's lifetimes continue to protect them in exchange for unquestioning loyalty[155]

In societies with a low level of individualism (collectivist societies), the relationship between people is highly important. People tend to stay in the same region and in the same community for their entire lives. Social networks are the primary source of information and problems, even very personal ones, are discussed within the own community. Harmony within society is a major goal. At the work place, teams rather than individuals are praised and rewarded for their performance. Collective interests in private life and at work are more important than individual demands. In individualist societies, the opposite is the case. People follow their own ideas and wishes. They are more mobile and therefore rather rely on media than on their community or family network to receive information. However, the personal business network plays an important role. It might even be larger than in collectivist societies but relationships are established for short periods of time and tend to be superficial. In societies that score high on individualism, everyone has and proclaims his or her own opinion. Individuals are rewarded for their performance based on goals that can be measured objectively. The entire relationship between employers and their employees is rather a contract on the labor market than a personal, family-like relationship. Autonomy and privacy are dominant ideals.

Masculinity (MAS)

> emotional gender roles are clearly distinct: men are supposed to be assertive, tough, and focused on material success, whereas women are

---

[155] See Hofstede and Hofstede (2005, p. 76)

supposed to be more modest, tender, and concerned with the quality
of life[156]

In masculine societies, people are striving for high earnings, advancements
on the career path and social recognition based on their achievements. They
enjoy challenges and always look for new ones. In class and at sports, compe-
tition is encouraged and everyone, especially boys and men, tries to excel. *"In
the family fathers deal with facts and mothers with feelings. [...] Boys play to
compete, girls to be together."*[157] On the contrary, in feminine societies, rela-
tionships play a more important role. Cooperation is more important at work
than individual performance. Social and employment security are necessary
for living a happy life. Both father and mother are responsible for family and
household and are encouraged to show their feelings. Men and women should
have similar ideals. Being ambitious, caring, decisive and gentle is associated
with both genders and not distributed between men and women. The align-
ment or unification of male and female tasks and ideals can be regarded as
ideal in feminine societies. There is no stereotype like 'boys play with cars
and girls with dolls' or 'men shop for cars and women for shoes'. Women and
men can study the same subjects and have similar jobs. Concerning state and
economy, economic growth is the ultimate goal in masculine societies. Femi-
nine ones rather pursue continuity and care for the environment. Masculine
societies support elites (survival of the fittest), feminine ones regard social
welfare as ideal. Simplified one can summarize, societies ranking high on mas-
culinity tend to support differences – between genders and also within one
group (only men or only women). Feminine societies value equality.

Uncertainty Avoidance Index (UAI)

the extent to which the members of a culture feel threatened by am-
biguous or unknown situations[158]

In strong uncertainty avoidance societies, people are often stressed and
highly anxious. They are afraid of ambiguous situations and risks in all parts
of life (family, work, etc.) and worry about health and money. Teachers should
have all answers and they inform rather than involve parents. Cars are bought
from well-known dealers and repaired by experts because used cars or home
repairs might involve risks. For the same reason, investments are often very
conservative and people can better be convinced by numbers than by feelings.
At work, employees tend to stay longer at the same company and clear tasks
are appreciated. In all parts of life (family, work and in society), strict rules
and precise laws are cherished. On the contrary, in weak uncertainty avoid-
ance societies, uncertainties are seen as an opportunity rather than a threat.

---

[156] See Hofstede and Hofstede (2005, p. 120)
[157] See Hofstede and Hofstede (2005, p. 132)
[158] See Hofstede and Hofstede (2005, p. 167)

People build their own houses and repair their own machines. They believe in doing everything themselves that they are able to do without external help. Risky investments are common because they hope for uncertain but potentially big returns. Since they do not fear the risk of becoming jobless or making a wrong choice, they often change jobs. At work, managers are responsible for the strategy. Daily operations are delegated because managers believe in motivation by transferred responsibility. People in weak uncertainty avoidance societies are good at creative processes and in pursuing innovative ideas. On the other hand, they dislike administrative work and implementation. They engage in society, are involved in politics, start associations and openly fight for their rights. Tolerance towards people who are 'different' is an ideal and even extreme ideas are fully accepted.

Long-term Orientation (LTO)

> the fostering of virtues oriented toward future rewards – in particular, perseverance and thrift. Its opposite pole, short term orientation, stands for the fostering of virtues related to the past and present – in particular, respect for tradition, preservation of 'face', and fulfilling social obligations.[159]

In long-term oriented societies, marriage is often considered a pragmatic arrangement. Living with in-laws is common and older children have authority over their younger siblings. They sometimes even take over responsibility for them. Success at school and work is attributed to efforts and investments in education are made early for paving the path to future success. Relationships (in personal and business life) are long-lasting and built over a long period of time.[160] A large savings quote and investments in real estate are very common. In short-term oriented societies, marriage is out of affection and living with in-laws is uncommon because it is regarded as a source of trouble. People do not want to age because the present moment is their main focus. Life only gets troublesome when growing older. Success is a matter of luck and can hardly be planned. Relationships are important for achieving certain things but friends and business contacts change over time. Creative thinking and personal freedom are highly important at work. Since short-term oriented people rather live in the present, they save little money and apartments and houses are rather rented than bought. People value their freedom and therefore do not want to bind themselves to a certain city or even their own property.

One of the advantages of Hofstede's model for comparing cultures is that it is dimensional (and not typological) and that he collected and published scores for each dimension for various countries.[161] It is therefore possible to compare

---

[159] See Hofstede and Hofstede (2005, p. 210)
[160] See also the Chinese concept of Guanxi, section 6.2.6
[161] See Hofstede and Hofstede (2005, p. 24)

the degree of cultural characteristics. A typological models, or a dimensional model without concrete value scores, only allows the assignment of certain characteristics to a culture without differentiating their magnitudes.[162] Hofstede's country scores enable researchers to cluster countries based on how they score on particular dimensions. Furthermore, dimensions can be combined and countries can be evaluated and compared in a matrix. This makes it easier to recognize correlations between dimensions and to combine insights from two or more dimensions. Hofstede's study has widely been criticized, mainly based on his selection of respondents (only IBM employees). However, it is still the most popular study in the field of intercultural research. It builds the basis for many other studies and provides practical insights for managers. A short discussion of Hofstede's work and its applicability for analyzing Chinese cultural characteristics is presented in section 6.1.5.

5.5.6 Fons Trompenaars and Charles Hampden-Turner

Fons Trompenaars, Dutch management trainer, business consultant and cross-cultural researcher, developed another dimensional model for identifying cultural differences. His model shows many similarities to Hofstede's work.[163] Fons Trompenaars was later joined by Charles Hampden-Turner and they together revised his ideas. In contrast to Hofstede, Trompenaars and Hampden-Turner use seven instead of five cultural dimensions.[164] Their model offers a slightly different view on cultural characteristics. As opposed to Hofstede, they not only include values that determine interpersonal relationships but also describe the behavior of people concerning time and their natural environment.

Trompenaars and Hampden-Turner published their ideas by jointly revising Trompenaars' most cited book *Riding the Waves of Culture: Understanding Cultural Diversity*.[165,166] Their time of writing (mostly 1990s) was most influenced by the understanding that culture is composed of *"shared values"* which is reflected in their work.[167] Trompenaars and Hampden-Turner have

---

[162] See section 5.5.1

[163] This is not surprising because Trompenaars is a scholar of Hofstede.

[164] See Trompenaars and Hampden-Turner (1997)

[165] See Trompenaars and Hampden-Turner (1997)

[166] Trompenaars and Hampden-Turner also wrote a couple of less well-known books *The Seven Cultures of Capitalism: Value Systems for Creating Wealth in the United States, Japan, Germany, France, Britain, Sweden, and the Netherlands* (Hampden-Turner and Trompenaars, 1993), *Building Cross-Cultural Competence: How to Create Wealth from Conflicting Values* (Hampden-Turner, Trompenaars, and Lewis, 2000), *Mastering the Infinite Game: How East Asian Values are Transforming Business Practices* (Hampden-Turner and Trompenaars, 2001) and *Managing People Across Cultures (Culture for Business Series)* (Trompenaars and Hampden-Turner, 2004).

[167] See Straub et al. (2002)

become most renowned because they do not analyze cultural dimensions for purely scientific reasons but put them into a managerial context and explore the impact of culture on business.[168] They compile insights from many other cultural researchers and adapt them to a management audience. Their work has not been as widely discussed and replicated as Hofstede's but gained considerable recognition, especially in the business world.

Out of the four popular dimensional models (Kluckhohn and Strodtbeck, Hall and Hofstede providing the other three), Trompenaars and Hampden-Turner's is the most recent one and is based on the findings of their colleagues. Since Trompenaars is one of Hofstede's former students, it is most similar to Hofstede's work.[169] Like Hofstede, Trompenaars developed an onion model for describing cultural differences (see figure 5.4, page 126). It exhibits a shift from the core to the shell – from implicit to explicit. The closer to the core a characteristic is, the more hidden it is from the outside world. *Basic assumptions* form the core and are strongest hidden from others. They are surrounded by *norms and values*, which are observable more easily. The shell is what other people often regard as cultural characteristics, *artifacts and products* (language, good, buildings, markets, fashion, art, . . .).[170]

Trompenaars and Hampden-Turner's dimensional model itself also shows many similarities to Hofstede's, including the way it was built. It consists of seven dimensions based on a quantitative analysis of 30,000 codified questionnaires,[171] distributed in a survey covering about 50 countries (including at least 100 respondents from each country).[172] Employees completing the questionnaire (mostly managers) had to decide between two or more different statements. Trompenaars chose this form of questionnaire because he believes in Edgar H. Schein's view of culture: *"Culture is the way in which a group of people solves problems and reconciles dilemmas."*[173] Both assume that cultural characteristics become particularly visible in dilemma situations. In contrast to Hofstede, Trompenaars' study did not focus on one particular company (IBM in Hofstede's case). Trompenaars worked with various companies covers numerous business fields. One could therefore argue that Trompenaars' research is more valid for describing national cultural because it is not biased by the corporate culture of a single company.

The seven dimensions Trompenaars and Hampden-Turner derived from their surveys are: *Universalism versus Particularism, Communitarianism versus Individualism, Neutral versus Affective, Diffuse versus Specific, Achievement versus Ascription, Time Orientation, Internal versus External Orientation.* Time orientation can be split into two separate dimensions, *orientations*

---

[168] See Kutschker and Schmid (2006, p. 726)

[169] Nevertheless, Trompenaars is also considered to be one of the strongest critics of Hofstede. See, for example, Smith, Dugan, and Trompenaars (1996)

[170] See Trompenaars and Hampden-Turner (1997, p. 20 ff)

[171] Hofstede's initial research relies on 116,000 questionnaires.

[172] See Trompenaars and Hampden-Turner (1997, p. 1 f.)

[173] See Schein (2004), referred to in Trompenaars and Hampden-Turner (1997, p. 6)

to past, present and future and *sequentially versus synchronically organized activities.*

Universalism versus Particularism (rules versus relationships)

Universalists focus more on rules than on relationships.[174] All people falling under the rule should be treated the same. Rule-based conduct has a tendency to resist exceptions. Universalists assume that exceptions weaken rules and that once you start making exceptions for illegal conduct the system will collapse. *Particularists* focus more on relationships than on rules. Their judgement embraces the exceptional nature of present circumstances. Each individual has a special relationship to me. I must therefore sustain, protect or discount this person no matter what the rules say.

Communitarianism versus Individualism (the group versus the individual)

Communitarianism manifests itself in *"a prime orientation to common goals and objectives"*.[175] The group is 'the end' and improvements in individuals capacities are means to that end. *Individualism* manifests itself in *"a prime orientation to the self"*.[176] The individual is 'the end' and improvements of communal arrangements are the means to support it.

Neutral versus Affective (the range of feelings expressed)

In *neutral* cultures, people do not telegraph their feeling but keep them carefully controlled and subdued. This does not mean that they are necessarily cold or unfeeling. The amount of feeling we show is often the result of conventions (or social norms). In *affective* cultures, people show their feelings plainly by laughing, smiling, grimacing, scowling and gesturing. They also tend to have a higher and often changing amplitude of voice. Touching other people, and the space we need between strangers without feeling invaded,[177] are other manifestations of differences between affective and neutral cultures.

Diffuse versus Specific (the range of involvement)

In *diffuse*-oriented cultures every life space and every level of personality tends to permeate all others.[178] It is the relationship between A and B that increases

---

[174] See Trompenaars and Hampden-Turner (1997, chapter 4)

[175] See Parsons and Shils (1951a)

[176] See Parsons and Shils (1951a)

[177] See Edward T. Hall (proxemics), 5.5.4

[178] Specific and diffuse cultures are equivalent to low and high context cultures. See Edward T. Hall, section 5.5.4

or reduces output, not the other way around (changed output does not affect the relationship). When dealing with diffuse-oriented people, expect them to be indirect and reserved. Logical reasoning does not convince them as long as you have not established a personal relationship. In *specific*-oriented cultures a manager segregates out the task relationship he or she has with a subordinate and insulates this from other dealings. Reputation is a characteristic that always leaks into other areas of life. The difference to diffuse-oriented societies lies in the extent (specificity: small, diffuseness: large). When dealing with specific-oriented people, expect them to be direct and precise. Logical reasoning is most important to convince them.

Achievement versus Ascription (how status is accorded)

In societies valuing *achievement*, status is accorded to people based on their achievements in the past. Achieved status refers to *doing*. In *ascription*-oriented societies, status is ascribed to people by virtue of age, class, gender, education, etc. Ascribed status refers to *being*.

Time Orientation

Trompenaars and Hampden-Turner describe two different concepts related to time. They both determine how we plan, handle and coordinate our activities. Since most of our activities are not restricted to our own enterprise but also affect clients, suppliers and partners, there are various cultural problems arising from differences in the conception of time.

- Orientations to past, present and future[179]
  Cultures can be clustered according to the importance they give to the past, present and future.[180]
- Sequentially versus synchronically organized activities[181]
  Cultures vary in their way of organizing activities. Some cultures regard time as sequential – a series of events happening in a particular order. They see time intervals as slots with the exact same length, organized one after another. Other cultures regard time as synchronic. Past, present and future are all interlinked and one can handle many activities at the same time. There is no concept like a *timeline*. Time is cyclical and repetitive.

---

[179] See Kluckhohn and Strodtbeck, section 5.5.3

[180] Saint Augustine expressed an interesting, but of course only his personal, view on those concepts: *"We live only in the present, but this present has several dimensions: the present of past things, the present of present things, and the present of future things."*, *"Your years are like a single day ... and this today does not give way to a tomorrow, any more than it follows a yesterday. Your today is Eternity."* Cited as in Shea and Huff (1995, p. 175) referring to Le Goff (1992, p. 3, 13). See also Neusner and Chilton (1997, p. 137) and Neusner (2004, p. 76)

[181] See Edward T. Hall, section 5.5.4, *Polychronic or Monochronic Time* (polychronic: synchronically organized, monochronic: sequentially organized)

Internal versus External Orientation (Do we control our environment or work with it?)

Inner-directed cultures (internal orientation) see nature as a system, a machine, that can be controlled by man. They are often based on Copernican or Newtonian ideas and try to measure their environment quantitatively. This inner-directedness is also present in the way managers from those cultures handle the business market and manage their own employees – regarding them as quantifiable resources.

External-directed cultures (external orientation) see themselves as part of their environment. They must go along with its laws, directions and forces and should learn to make use of them by aligning their own goals with the opportunities the environment offers. Long-term orientation and harmony are important principles in those societies.

Trompenaars' seven dimensions can be divided into two sets. The first set consists of five dimensions and focuses on *human relationships*. The second one describes the relation of humans to two external factors – *time* and *environment*.[182] The first set is aligned with Talcott Parsons' research,[183] the other two dimension are adopted from Kluckhohn and Strodtbeck.[184,185]

There is some criticism concerning Trompenaars' methodology and his dimensions. Trompenaars ranked countries and analyzed their cultural characteristics based on the statements of his survey participants. In contrast to Hofstede, Trompenaars did not aggregate statements focusing on the same dimension. He therefore did not derive scores for each of his seven dimensions. Trompenaars rather evaluated the survey results for each of his questions consecutively. It is therefore not possible to draw an exact graph based on Trompenaars' research that shows cultural differences between countries for each dimension. Kutschker and Schmid assume that Trompenaars' dimensions are not atomic and consist of different sub-dimensions.[186] This might be a reason why Trompenaars did not derive exact rankings but only shows the relative position of different countries for each of his questions. There is other criticism from researchers concerning Trompenaars' approach. It is, for example, often criticized that Trompenaars did not ground his dimensions in data but rather based them on existing literature. Trompenaars does not explain how he chose the dimensions which he integrated into his model. His dimensions might not exhaustively describe cultural differences and are likely to overlap. Furthermore, the selection of participants has an effect on the results that is not discussed thoroughly. A big share of respondents are

---

[182] I would further divide Trompenaars' time dimension. That would lead to eight independent dimensions.
[183] See section 5.5.7 and Parsons (1991)
[184] Those are the aspects *time* and *environment*. See section 5.5.3
[185] See, for example, Hofstede and Hofstede (2005, p. 379)
[186] See Kutschker and Schmid (2006, p. 734)

professionals who attended his intercultural trainings. Those participants certainly have been thinking about or have recently experienced intercultural clashes. They have therefore reflected their own culture which might have influenced Trompenaars' results. On the other hand, many practitioners support Trompenaars' approach. They value its comprehensibility and the focus on the business impact of intercultural differences. Moreover, in contrast to Hofstede, Trompenaars' respondents worked in different companies and a particular corporate bias, like it might be inherited from IBM's corporate culture in Hofstede's study, is less likely. Stronger than Hofstede, Trompenaars acknowledges and attempts to highlight differences within countries. He does not restrain his model and his results to national cultures but also relates to corporate, professional and gender differences in cultures.

5.5.7 Other Researchers and Models

There are various other researchers who built their own cultural models or refined one of those we already discussed. I cannot present all of them here but I will introduce those researchers (and their models) who influenced my thinking during the process of research and while writing this thesis. The exclusion of others does not delimit their importance in general. The following researchers were those who had a direct influence on the outcome of this thesis. Introducing these researchers is important for understanding the relations between different movements in cultural research, the context of a few remarks I will make later on and the decision which cultural models to build my thesis on. The busy reader who is not interested in background information about cultural models can skip this section and directly continue with chapter 6.

Talcott Parsons: Pattern Variables

Talcott Parsons,[187] one of the most renowned sociologists in the 20th century, is best known for his *grand theory*. This theory is an attempt to create a framework that covers all social sciences. It has been widely acknowledged during the 1940s and 50s until the 1960s. After his ideas were abandoned for about 20 years, his theory experienced a revival. It came into the focus of research in the 1980s again and is still actively discussed today.[188]

His most cited publications are one of his first works, *The Structure of Social Action*,[189] and a compendium, *Toward a General Theory of Action*,[190] which he edited together with Edward A. Shils.

By integrating all social sciences into a holistic framework, Parsons could analyze human behavior from various different perspectives. He defined a set

---

[187] Talcott Parsons was born in 1902 and died in 1979.
[188] See Treviño (2001, p. xv)
[189] See Parsons (1949)
[190] See Parsons and Shils (1951a, 2001)

of five dichotomies – also called *pattern variables* – *"that may be used to categorize actors' orientation in the personality system, the value patterns of the cultural system, and normative requirements in the social system"*:[191,192,193]

- Affectivity vs. Affective Neutrality
- Self-orientation vs. Collectivity-orientation[194]
- Universalism vs. Particularism
- Ascription vs. Achievement
- Specificity vs. Diffuseness

Parsons himself writes about the origin and applicability of his pattern variables: *"The pattern variables first emerged as a conceptual scheme for classifying types of roles in social systems, starting with the distinction between professional and business roles. [...] In Towards a General Theory, the scheme was substantially revised and its relevance extended from role-analysis in the social system to the analysis of all types of systems of action."*[195] Even though Parsons suggests the application of his pattern variables to systems other than social systems, they have mainly been used for analyzing societies (and cultures). His pattern variables provide the basis for a classification scheme for norms and values in societies. By analyzing norms and values, a fit of those two can be examined and tensions in society can be discovered.

Shalom H. Schwartz

Social psychologist and cross-cultural researcher Shalom H. Schwartz developed own value systems which are praised by many renowned researchers worldwide, including Geert Hofstede.[196] Schwartz, as many others, defines values as the desirable that leads people in their lives. His value systems were developed for two purposes (and therefore focus on two levels) – the comparison of individuals and societies.

His three main works are: *Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries*,[197] *Beyond Individualism/Collectivism: New Cultural Dimensions of Values*[198] and *A Theory of Cultural Values and Some Implications for Work.*[199]

---

[191] See Treviño (2001, p. xxxviii)

[192] There was a interesting debate between Robert Dubin and Talcott Parsons on Parson's model. I restrain from presenting this debate here but recommend a read of two of their papers for gaining deeper insights. See Dubin (1960) and Parsons (1960)

[193] For a list of his five pattern variables, see, for example, Hofstede (2001, p. 30)

[194] Parsons later dropped this pattern variable. See, for example, Treviño (2001, p. xli) and Hofstede (2001, p. 49)

[195] See Parsons (1960, p. 467)

[196] See Hofstede (2003, p. 220 ff) and Hofstede and Hofstede (2005, p. 32)

[197] See Schwartz (1992)

[198] See Schwartz (1994)

[199] See Schwartz (1999)

The value systems by Schwartz builds the basis of two influential studies. First, he is involved in and his systems are used for the European Social Survey which scrutinizes differences in European cultures.[200] Second, *Culture, Leadership, and Organizations. The GLOBE Study of 62 Societies* derives many values from Shalom Schwartz and Geert Hofstede. The GLOBE Study continuously compares its findings to those by Schwartz and Hofstede and states correlations.[201]

Ronald Inglehart: World Values Survey

Ronald F. Inglehart, a US American political scientist, is best known for his work on value shifts. He is the chairman of the executive committee of the *World Values Survey*. With his background in politics, he offers a new perspective on cultural values. Inglehart's theory of how value shifts occur was heavily influenced by Abraham Maslow's *hierarchy of needs*. In order to understand Inglehart's work, we need to take a short look at Maslow's model.[202] It is presented as figure 5.13.

Excursus: Maslow's Hierarchy of Needs

Maslow's original pyramid consists of five levels of needs: *Physiological*, *Safety*, *Social*, *Esteem* and *Self-Actualization*. Those needs can be grouped into two categories, deficiency needs (D-needs) and being or growth needs (B-needs). The first group of needs, deficiency needs, must always be satisfied. Without a satisfaction of those needs, humans suffer. They feel an inner tension and might even react physically to their unsatisfied needs. These D-needs have a specific order in which they must be satisfied. If physiological needs are not met (breathing, food, sleep, etc.) all of our energy goes into remedying those deficiencies. As a consequence, we do not react to those needs higher in the hierarchy. If a need is fulfilled, we realize the demand for the next one but do not draw any further motivation out of the satisfaction of lower ones. If all deficiency needs are met, the deficiency is remedied and we are satisfied. This is when growth needs (B-needs) surface. B-needs, like the need for self-actualization (personal growth and fulfillment), can motivate us without any particular border. Besides self-actualization, Maslow also mentions *cognitive needs*, *aesthetic needs* and *transcendence needs*.[203] These needs can all be

---

[200] *"The European Social Survey (the ESS) is an academically-driven social survey designed to chart and explain the interaction between Europe's changing institutions and the attitudes, beliefs and behaviour patterns of its diverse populations. Now moving into its fourth round, the survey covers over 30 nations and employs the most rigorous methodologies."* For more information see `http://www.europeansocialsurvey.org/`

[201] See section 5.5.7 and House et al. (2004)

[202] See Maslow (1943)

[203] See Maslow (1993) and Maslow (1998)

categorized as growth needs (B-needs) and as thus be integrated into Maslow's pyramid. B-needs can hardly be met so that we are afterwards satisfied for the rest of our lives but rather grow together with us.

Fig. 5.13. Maslow's Hierarchy of Needs

Even though Maslow is certainly not the focus of this thesis, his ideas, especially combined with Inglehart's theory of value shifts, provide valuable insights into current developments in China. Some cultural values seem to be shifting in China right now due to rapid social and economic progress. This makes China hard to analyze in terms of value orientation. As soon as deficiency needs are met, which is still not the case in many parts of China, growth needs come into play. The realization of growth needs can be accompanied by a shift in values which need to change in order to meet the needs. Even though values change slowly, rapid changes in society can speed up the process.

Inglehart's Theory of Value Shifts

The name Ronald Inglehart is directly linked to the concept of *post-materialism*. Most notably, the concept of post-materialism is described in *The Silent Revolution*.[204] Based on Maslow's hierarchy of needs, Inglehart proclaims that humans pursue goals in a particular order and that their values change according to their actual needs.

Since many societies have recently experienced social stability for the first time, their needs shift accordingly. Before that shift, the focus was on assuring pure survival, safety, defense, etc. Nowadays, with growing materialistic freedom, large parts of many societies regard personal development, individuality and personal freedom as highly important. According to Inglehart, many societies have entered a period of post-materialism.[205]

---

[204] See Inglehart (1971, 1977)
[205] See, for example, Inglehart (1990) and Inglehart (1997)

However, there are also backlashes. The need for law and order, as it was present in the United States in the 1970s and 1980s, dominated most growth needs which were higher on the Maslow pyramid. The fulfillment of the needs for law and order had an immense effect on political decisions. The same can still be seen as valid today. After the terrorist attacks in September 2001, the need for security was dominating the US American society again. Countermeasures were introduced that have violated civil rights and in some cases even human rights. In the last couple of years, as national security seems to be rather stable and the fear of terrorist attacks has declined, growth needs play a highly important role again.[206]

Inglehart's insights can also be used to observe and understand social trends within countries. Shifts in the German society after the German reunification can for example be observed. From 1980 to 1990, the share of post-materialists in the Federal Republic of Germany increased from 13 to 32 percent. This can easily be explained as an effect of the German *Wirtschaftswunder*. Surprisingly, after the German reunification in 1990, the trend turned and the percentage of post-materialists dropped significantly (1990: 32 %, 1992: 23 %).[207]

Inglehart conducted a series of studies in order to show those value shifts and to analyze the status quo in various societies all over the world. In order to receive realistic results, he compared political values of age cohorts (people born around the same period) living in different countries.[208] The most renowned study that is based on his value system is the *World Values Survey*. It is a worldwide survey which is repeated regularly. Most results of the survey are presented online on the projects website.[209] Inglehart uses many different values for observing value shifts in his target societies. However, as a result of his studies, he summarizes that two main dichotomies are sufficient to broadly describe cross-cultural variations: *traditional vs. secular-rational* and *survival vs. self-expression*. Inglehart states that those two factors sufficiently describe cross-national variance and that they correlate with most other variables. Obviously, one dichotomy (survival versus self-expression) represents different stages of a society on Maslow's pyramid. Combining those two insights – Inglehart's two main dimensions correlate with most other cultural values and at least one of those two dimensions is based on Maslow's hierarchy of needs – is seems likely that cultural values change with social and economic

---

[206] Recently, the financial crisis has shook the United States. This crisis has the potential to turn the trend so that deficiency needs will gain importance once again, as citizens loose their jobs and homes.

[207] See Terwey (2000, p. 154 ff.)

[208] See Eagles, Johnston, Johnston, and Holoman (2003, p. 159)

[209] See http://www.worldvaluessurvey.com/. Inglehart summarizes recent insights in Inglehart (2004).

progress.[210] Especially due to China's rapid rise, this should be considered when reviewing China's cultural scores.

Robert J. House et al.: The GLOBE Study

The GLOBE Study, is the most profound study of cultural differences that has been developed in recent years.[211] By its team's own account, the GLOBE research project has been compiled for a period of 10 years, from 1994 to 2004. 170 investigators worked on the project, analyzing 62 societies by collecting data from 17,300 managers in 951 organizations.[212] The focus of the GLOBE Study lies on leadership and differences in leadership in different societies, but it also analyzes other cultural, societal and organizational characteristics in 62 societies.[213]

The GLOBE Study is mainly based in three cultural models and the work of their researchers: *Kluckhohn and Strodtbeck*, *Hofstede* and *Inglehart*. This applies to its research methodology but also to the choice of variables.[214] For analyzing cultural characteristics, it uses nine dimensions, reflecting those of the mentioned researcher:[215] *Future Orientation*, *Gender Egalitarianism*, *Assertiveness*, *Humane Orientation*, *In-Group Collectivism*, *Institutional Collectivism*, *Performance Orientation*, *Power Distance* and *Uncertainty Avoidance*. For analyzing leadership, the research team identified six global leadership dimensions: *Charismatic/Value-Based Leadership*, *Team-Oriented Leadership*, *Participative Leadership*, *Humane-Oriented Leadership*, *Autonomous Leaderhsip* and *Self-Protective Leadership*.

Besides the explicit focus on leadership, which was a new aspect that had not been analyzed in depth before, the major difference to earlier studies was that the GLOBE research team split their scales into how managers actually work (practices) and how they believe good leadership in their organization should look like (values). They further analyzed practices and values in the societies of those managers. This split between values and practices as well as between organizations and societies is unique and provides valuable insights.

In this thesis, the content of the GLOBE Study cannot be presented in depth. However, it was a precious source of inspiration and further helped

---

[210] For more information on the link between cultural values and modernization as well as economic progress, see Inglehart and Baker (2000).

[211] The GLOBE Study is primarily driven by Robert J. House, the founder of the project.

[212] See House et al. (2004, p. xv) and Chhokar, Brodbeck, and House (2008)

[213] The core questions the study addresses are listed on page 10 of House et al. (2004).

[214] Even though these researchers had the biggest impact on the study, there are many other researchers who also had an influence. One dimension (In-Group Collectivism) is for example derived from Triandis (1995) and another one (Performance Orientation) from McClelland (1961).

[215] See, for example, (House et al., 2004, p. 3 or p. 11 ff.)

reflecting the dimensions of other researchers, Hofstede's dimensions in particular.

Missing Researchers

There are many influential and renowned researchers in the field of cultural studies who I have not mentioned yet and who might only be addressed in a footnote in the course of this thesis. Since this thesis is not meant to provide an all-embracing description of the status quo of intercultural research but focuses on the impact of culture on information security, I have only introduced those researchers that are necessary for understanding the rest of this thesis. Nevertheless, I believe that I have provided a holistic view on intercultural research and covered the most important researchers in this field.

The interested reader can further deepen his knowledge by reviewing *Inkeles and Levinson: 'National Character: The Study of Modal Personality and Sociocultural Systems' and 'National Character: A Psycho-social Perspective'*[216], *Condon and Yousef: 'An Introduction to Intercultural Communication'*[217], *David A. Victor: 'International Business Communication'*[218], *Quincy Wright: 'A Study of War'*[219] and *Richard D. Lewis: 'When Cultures Collide: Leading Across Cultures'*[220]. For understanding the roots of intercultural research and for reviewing early ideas on the role of culture in shaping human life, Ruth Benedict's *Patterns of Culture*[221] is probably the best read. Nancy J. Adler sensitizes professionals for intercultural issues with publications like *From Boston to Beijing: Managing with a World View*[222] and bridges the gap between theory and practices by applying dimensions of value orientation by Kluckhohn and Strodtbeck, Hofstede, etc. to management practices. Her book *International Dimensions of Organizational Behavior*[223] is an excellent introduction to intercultural issues and their impact on corporate management.[224]

Of course, also this list cannot be exhaustive and can only provide further inspiration. For more information, please refer to the references I provided and enjoy plunging into the field of intercultural research.

---

[216] See Inkeles and Levinson (1969, 1997)
[217] See Condon and Yousef (1985)
[218] See Victor (1992)
[219] See Wright (1983)
[220] See Lewis (2005)
[221] See Benedict (1989)
[222] See Adler (2001)
[223] See Adler (2002)
[224] For more work by Nancy J. Adler, see Adler (1983a,b); Adler, Doktor, and Redding (1986)

5.6 Concluding Remarks

In former chapters, we realized that the human factor plays a major role in information security. First researchers have started merging concepts from economics and psychology with information security. However, cultural aspects have largely been neglected up to now. For analyzing the impact of culture on information security, research needs to be based on a sound fundament. This fundament can only be built by deepening our understanding of cultural studies. This chapter started with a brief overview of the human factor in information security and the distinction between security cultures and the impact of culture on information security. Security cultures can be seen as corporate cultures that embrace secure behavior. They are used by security managers as a regulator to raise the security level in their companies. The impact of culture on information security should rather be seen as the opposite – a security threat induced by cultural characteristics.[225] Those cultural characteristics can have very different scopes. There can be part of regional, national, professional, corporate, gender cultures and many more. The main focus of this thesis lies on national cultures. With a sound fundament in cultural studies, they can be analyzed systematically and generate highly valuable and generic results that security managers and risk managers can use for their daily work. Regardless of its scope, every kind of culture can be described as an onion. The layers close to the core are invisible to outside observers, outer layers can be examined more easily. Cultural values are at the core of the cultural onion. They are established early in life and change only slowly. This is one of the reasons why many dimensional models are based on values. But dimensional models that describe cultural values, which respectively determine the behavior of members of a cultural group, provide only one perspective on intercultural issues. The second branch of cultural studies is intercultural communication.[226] Miscommunication, as well as the behavior of individuals, is also often rooted in conflicting cultural values. However, research in the field of intercultural communication describes problems that occur when there is a cultural gap between two parties. As mentioned above, dimensional models can also be used for describing the behavior of individuals (based on values), regardless of other parties. For both branches of cultural studies, the most important researchers and their cultural models were introduced. These models will be used as the the stable fundament that I demanded at the end of the last and the beginning of this chapter. In the course of this chapter, we did not become intercultural experts but became familiar with the necessary concepts, methods and tools that we need for analyzing the

---

[225] Of course, some regional and professional cultures also support information security efforts and raise the security level. However, the ones that create security threats are more important to us because we have to protect our corporations against those threats.

[226] Research on intercultural communication can also make use of dimensional models.

impact of culture on information security. In the next chapter, we will use these tools and will create another jigsaw piece for reducing the information asymmetry between managers and their employees as well as companies and their outsourcing providers. We will continue our journey to understand how culture affects information security.

6

Culture and Information Security

With a solid fundament – a proper understanding of concepts, methods and tools from the field of cultural studies – we can start analyzing the impact of culture on information security. This chapter is devoted to an analysis of cultural characteristics and the presentation of related security threats. The findings are based on the interviews that I conducted in the Chinese outsourcing sector. These findings are generalized and are used as input for a model that can predict security threats and compare the security level of countries purely based on their cultural characteristics. This chapter reduces the gap between information security and cultural studies.

6.1 Introduction

Information security in general, and outsourcing relationships in particular, are influenced by various factors. In chapter 4, we saw that the country selection plays an important role for outsourcing decisions because of environmental factors like economic, social and political stability, legal regulations, corruption, etc. We also realized that we need to look into social sciences in order to understand potential security threats on the levels of the individual and the group. Therefore, I introduced researchers from the field of cultural studies and their work in the previous chapter. Their research builds the basis that we need for analyzing the impact of culture on information security.

As we saw in chapter 5,[1] the human factor (cultural characteristics in particular) plays an important role in information security. However, its influence has hardly been analyzed up to now. I conducted qualitative exploratory research for understanding information security issues that arise when outsourcing IT services in or to the People's Republic of China. Based on the results of my problem-centered interviews,[2] I link cultural characteristics with security issues that correlate with these characteristics. Therefore, I go through a

---

[1] See especially section 5.1
[2] See appendix A

selected set of cultural characteristics and highlight security threats that are related to each characteristic. Throughout the chapter, I provide anecdotal evidence in form of small case studies[3] to illustrate the findings. Furthermore, I analyze characteristics and related threats on an abstract level so that the results can be generalized and used for analyzing other countries. While presenting my findings, I triangulate with other research fields to validate my results.

A risk manager can look at the cultural characteristics prevalent at his outsourcing destination of choice. By reviewing the relevant section of this thesis, he gets an idea of what kinds of security threats might arise as a result of this cultural characteristic. At the end of the chapter, I assess the impact of every cultural characteristic and build a model that can be used to determine the intensity of culture-based security threats in certain societies. This model can be used for analyzing the likelihood and the impact of security incidents. It can be seen as a first attempt to rank the security risk of outsourcing destinations based on their cultural characteristics.

6.1.1 Methodology

For analyzing the influence of culture on information security, I followed a qualitative exploratory research approach. This approach is described in detail in appendix A. This section explains how I use anecdotal evidence and triangulate with a field similar to information security – air traffic safety.

In the last chapter, I introduced a large number of cultural researchers and their work. This was necessary to deepen our understanding of human behavior and to understand different ways of analyzing cultures. In this chapter I reduce the number of researchers and select two of them, together with their cultural models. In section 6.1.4, I describe how and why I selected these researchers and their cultural dimensions. Their dimensions are used to cluster my findings and to provide a model that can be used by information security and risk management professionals facing the outsourcing decision. Based on the selected dimensions, this chapter introduces the research findings which I made on the level of the individual and the group.

6.1.2 Anecdotal Evidence and Case Studies

Anecdotal evidence can be seen as a tool for gaining insights by providing examples of generic concepts. The term also sometimes refers to evidence that is untrustworthy or based on wrong reasoning. I would like to stick to the first meaning and define anecdotal evidence as short samples of case studies. Whereas case studies normally provide a relatively holistic picture of a situation, anecdotal evidence is used for presenting specific insights. Anecdotal

---

[3] See section 6.1.2

evidence can be used for generating new hypotheses but cannot prove an existing one. Like a testimony in front of a court, anecdotal evidence can be scrutinized and its validity tested.

The anecdotal evidence in this chapter is presented in form of short case studies from the outsourcing industry.[4] I present those cases in order to stress points that I make. They also provide examples that make it easier to understand the results that I describe on a rather abstract level. Regarding the trustworthiness (credibility, transferability, dependability and confirmability) of my work, please refer to section A.1.1. I hope that you, as my reader, find the use of anecdotal evidence valuable and that it enriches your understanding of the influence of culture on information security.

6.1.3 Triangulation with Air Traffic Safety

If an airplane crashes, the outcome is likely to be lethal for most passengers. Therefore, this field has been analyzed by numerous researchers from various different perspectives. Commercial aviation statistics indicate that human error is the cause of the majority of all accidents. Technical failures play a less important role.[5,6] Three factors emerged throughout various studies: *Communication and Coordination*, *Command Responsibility* and *Recognition of Stress Factors*.

In the following, we will take a look at the influence of national cultures on air traffic safety for two reasons. First, by reviewing literature in this field, we will see that Hofstede's dimensions can be applied to analyze safety and security issues.[7] Second, and maybe even more important, since safety and security are highly interlinked and similar concepts, we might find analogies that can deepen our understanding of the influence of national culture on safety and security.

Talking about air traffic safety, it is important to understand the difference between *security* and *safety*. Security is the protection against danger and loss. From an information security perspective, it is the protection of data from getting disclosed (confidentiality), altered (integrity) and lost or becoming

---

[4] For more information on qualitative case studies, see Stake (2005)

[5] Kjell Mjøs refers to statistics by Boeing which identify human error as the cause of more than 70 percent of all accidents. See Boeing (1996) as cited in Mjøs (2004, p. 151). Boeing regularly publishes a *Statistical Summary of Commercial Jet Airplane Accidents*. Unfortunately, the most recent issue does not provide any data on the causes of accidents. See Boeing (2008)

[6] However, one should also keep in mind that people are often blamed for making mistakes that can be attributed to design flaws. If systems were designed better, many *human errors* could be circumvented. Donald A. Norman published an entire book devoted to *The Design of Everyday Things* and common design flaws. See, for example, Norman (1998, p. xviii and p. 44)

[7] As described later on, his dimensions are still applied and replicated today, decades after Hofstede first developed his model.

temporarily unavailability (availability). The term security is normally used when someone actively engages in the protection of something against threats from outside (like malicious intruders).[8] Safety, on the other hand, refers to the state of being protected against any kind of external harm that is not caused by somebody else deliberately. A failure of a machine that causes injuries or death is an example of insufficient safety. This distinction is not always made properly. The borders between security and safety blur. There is another common way of differentiating between security and safety that might be easier to use. Security is often used for objects (like data), safety for the protection of human beings.

In the context of aviation, both terms *safety* and *security* or *aviation safety* and *aviation security* respectively, are described by Boeing as follows:[9]

> Aviation safety refers to the efforts that are taken to ensure airplanes are free from factors that may lead to injury or loss.

> Aviation security is only one component that may affect passenger safety. It is not so much related to the airplane itself, but rather to intelligence gathering, pre-boarding procedures and airport security personnel. It is mainly aviation security that has been receiving urgent attention since Sept. 11.

Even though there are major differences between security and safety, the two concepts also exhibit many similarities. Both refer to the state of being protected against something. Both kinds of risk, safety and security risks, can be measured and managed. If the risk is underestimated, losses exceed the benefits (usually saved costs) of not implementing a particular security or safety measure. The field of air traffic safety can be regarded as an example of almost zero tolerance. An airplane must at least be protected against all kinds of threats that cause it to crash. The similarities between security and safety suggest to review research in the field of air traffic safety for potential analogies.

Hofstede's Cultural Dimensions and Air Traffic Safety

We discussed Hofstede's cultural model earlier in this thesis[10] and we will further use his dimensions in the course of this chapter.[11] Hofstede is probably the most renowned cross-cultural researcher and there are various studies in

---

[8] Outside does not necessarily refer to somebody outside of the organization but to external threats that are imposed on the organization intentionally. When talking about security, somebody usually wants the organization to be unsafe.

[9] See   http://www.boeing.com/commercial/news/feature/safety.html [10.08.2008]

[10] See section 5.5.5

[11] See next section 6.1.4

other fields that replicate Hofstede's cultural dimensions. The field of air traffic safety is one of those fields. Robert Helmreich and Ashleigh Merritt, for example, collected data from more than 9,000 commercial pilots worldwide and prove a significant correlation between their data and Hofstede's first four dimensions (Individualism-Collectivism, Power Distance, Masculinity-Femininity and Uncertainty Avoidance).[12] Furthermore, there are many specialized studies focusing on countries (for example Mjøs (2004) analyzing three Norwegian airlines or Yong (2003) focusing on Taiwan's civil aviation), particular sectors (e.g. military aviation, see Soeters and Boer (2000)) or even certain programs (e.g. the Royal Canadian Air Cadet Gliding Program, see Dutcher, Carrick, and Smith (2002)). Those studies not only replicate Hofstede's findings, they also associate particular cultural characteristics with a higher or lower risk of human error in aviation.[13] One result is for example that a strong tendency towards *Collectivism* and high *Power Distance* has a negative impact on air traffic safety. An example that is often described is the inability of co-pilots to criticize their pilots if they come from high power distance countries. Even in critical situations, the pilots' mistakes are not addressed which causes serious safety risks. Some studies provide suggestions and describe methods how to resolve those safety issues. I will not elaborate on the findings of these studies here but rather present similarities when focusing on particular cultural dimensions and their influence on information security.

Some authors have argued that cultural differences might vanish due to the emphasis on modernization and technical advancement of the pilot profession. However, research shows that differences between national cultures still play a dominant role in aviation safety. Replication studies like the ones mentioned not only underline the validity of Hofstede's approach but also highlight the applicability of his dimensions in the field of air traffic safety. Furthermore, they provide analogies that can be used for underlining the importance and the validity of this thesis.

Communication and Air Traffic Safety

Communication plays a highly important role, both for security and safety. In aviation, problems in communication can have deadly consequences. Mis-

---

[12] See Merritt and Helmreich (1996), Sherman, Helmreich, and Merritt (1997), Merritt (1998) and Merritt (2000)

[13] Concerning the replication of Hofstede's findings, most authors highlight that some characteristics (e.g. high power distance and strong individualism) are reinforced by the professional culture in the aviation industry and organizational cultures. However, they also find the same cultural differences between countries that Hofstede identified. The pilot profession, regardless of its emphasis on modernization and technological advancements, does not neutralize cultural differences. See Merritt and Helmreich (1996, p. 11)

communication can happen on various levels. It can be based on differences in national cultures but this is not necessarily the case.

Language barriers can lead to miscommunication. An incident (happening in June 2007) in which the crew of a Lot Polish Airlines Boeing 737-500 struggled to communicate with British air traffic controllers is described by Linda Werfelman in *AeroSafety World*.[14] When the displays of the aircraft's electronic instruments went blank, the crew had to communicate with air traffic controllers and resolve the problem at the same time. Even though both pilot and co-pilot had sufficient professional experience (15 years and 6 years of experience with the same type of aircraft), they struggled with the instruments. This might have handicapped the communication with controllers but the real problem was the Polish crew's low proficiency of the English language. Proficiency standards by the *International Civil Aviation Organization (ICAO)* required an operational level of the English language as of March 2008.[15] However, the example describes a situation in which communication on an *operational level* was not enough and the need for *plain English* arose.

Language problems can even be intensified by cultural characteristics. An example can be presented by briefly reviewing the concept of *face* which is deeply rooted in various Asian cultures. Face is something that a person possesses. It can be similar to prestige or social relations but can also stand for a moral character. It can be given, taken away and lost – for example when one does not come up to the expectations of others. I recently talked to consultants in the air traffic industry and they told me that incidents with Chinese pilots often occur due to their poor English skills and that these problems are amplified by their fear of loosing face. If they encounter problems communicating with air traffic controllers, they might not ask for clarification because this would show their lack of proficiency in the English language. They would thereby loose face because as pilots on international flights they are expected to be able to communicate in English. This is just one example of the impact of culture on air traffic safety.

Learning from Analogies

Reviewing studies in the field of air traffic safety reveals that human error is the dominant cause of accidents. Particular cultural characteristics and intercultural differences play a significant role. These findings and the similarities of safety and security suggest that also in the field of information security, the impact of culture should not be underestimated. Hofstede's dimensions and Hall's findings on intercultural communication are useful for analyzing culture-related safety and security threats. By reviewing culture-related safety threats in the aviation industry and analyzing how safety managers minimize risks,

---

[14] See Werfelman (2008)

[15] The deadline was postponed to March 2011 because many member states did not manage to adhere to it.

we can learn how to solve security problems in outsourcing relationships. The analogies between air traffic safety and information security are considerable and provide invaluable insights.

6.1.4 Selected Dimensions: Geert Hofstede and Edward T. Hall

In the last chapter, I reviewed the work of many prominent cultural researchers. For a deeper analysis of the impact of culture on information security, it is neither necessary nor advisable to use all dimensions that were introduced. On the contrary, by focusing on fewer dimensions, these can be analyzed in depth. Furthermore, by reviewing the cultural researchers I introduced, it becomes clear that their work – and thereby their dimensions – overlap to a large extent. Reducing the number of cultural characteristics also ensures that findings are not presented twice.

The decision which dimensions to include in the study was difficult and not straightforward. My first approach was to list all dimensions and reduce the list to a few dimensions that are *MECE* (mutually exclusive and collectively exhaustive). However, I soon realized that the dimensions only partially overlap and a list of mutually exclusive (non-overlapping) dimensions would be hard or even impossible to compile. If one followed this approach, many special aspects of individual dimensions would have been neglected because dimensions had to be excluded from the list due to certain overlaps with other dimensions. Even though many cultural researchers have entered this endeavor, it does not seem possible to compile a list of cultural characteristics that is mutually exclusive or collectively exhaustive. Cultural characteristics are always interlinked and they can never describe all aspects of a particular culture. Selecting dimensions from different cultural researchers would have further complicated the analysis because different researchers collect, evaluate and describe their dimensions differently. A coherent analysis based on those dimensions would have been highly complex – if not impossible.

Focussing on the goal of this thesis, to explore the impact of culture on information security, it becomes obvious that a mutually exclusive and collectively exhaustive set of dimensions is not necessary. By exploring cultural dimensions, even if they are not collectively exhaustive,[16] the relation between culture and information security can be shown and further research motivated. The selected dimensions can be analyzed in depth and this analysis can be used and built upon by researchers and practitioners alike.

During the data collection period, two main requirements for selecting cultural characteristics that should be scrutinized further became apparent:

- There are two kinds of security incidents that can be attributed to cultural characteristics. Some security threats are based on the behavior of a single individual. This behavior is partially due to his or her cultural

---

[16] and also not mutually exclusive

background. The background of an employee can imply certain (sometimes security-relevant) behavior. The other form of security threats arises if two parties with different cultural background cooperate. Frequently, intercultural clashes occur. Besides the behavior of a single employee, these intercultural differences can also lead to security threats. These threats are partly but not solely due to miscommunication. Cultural characteristics that were selected for further analysis should cover these two fields of intercultural research.

- The second requirement is that the cultural characteristics chosen should be thoroughly reviewed by the international research community. Thereby, potential weaknesses of these characteristics are well-known and can be anticipated.

These two requirements led me to focus on the cultural dimensions defined and analyzed by Geert Hofstede and Edward T. Hall. Geert Hofstede is the most prominent cultural researcher focusing on national cultural characteristics. His research has been reviewed and critiqued for decades and no current research study on national cultures can neglect Hofstede's findings. His five dimensions[17] are neither mutually exclusive nor collectively exhaustive but they cover a large spectrum of cultural characteristics. Edward T. Hall, on the other hand, focuses on intercultural encounters. He has influenced research in the field of intercultural communication like no other researcher and, as for Geert Hofstede, many cultural researchers have built upon his findings.

The second requirement, the review by the international research community, can easily be probed by comparing the number of citations of major intercultural publications in Google Scholar.[18] One can argue that Google Scholar is not a valid source because it might not index all references. However, it can support the argument that both researchers, Hofstede and Hall, can be seen as most influential in their fields. Table 6.1 shows the number of citations of the most important publications of various cultural researchers. All of them could be built upon for analyzing the impact of culture on information security. The data was collected on July 10th 2008. It is aggregated in figure 6.1.

These citation numbers show that Hofstede and Hall are the two most renowned researchers in the field of intercultural research. Hofstede's cultural dimensions describe culture as part of each individual. It is specific to a group of people and can be observed by comparing the behavior of its members to the behavior of another cultural group. Cultural characteristics are learned throughout our lives and are based on experiences. They are internalized by individuals and groups. Hall, on the other hand, provides a comprehensive model for analyzing intercultural communication. His dimensions play a major role when two individuals with different cultural backgrounds interact. Thereby, Hofstede and Hall offer two distinct views on different phenomena,

---

[17] See section 5.5.5
[18] See http://scholar.google.com/

Researcher	Publication	Citations
Geert Hofstede	Culture's Consequences	13077
Geert Hofstede	Cultures and Organizations	6864
Edward T. Hall	The Hidden Dimension	2191
Edward T. Hall	The Silent Language	2143
Edward T. Hall	Beyond Culture	2002
Edward T. Hall	Understanding Cultural Differences	696
Edward T. Hall	The Dance of Life	625
Edward T. Hall	Hidden Differences	287
Fons Trompenaars	Riding the Waves of Culture	2322
Fons Trompenaars	Seven Cultures of Capitalism	519
Kluckhohn & Strodtbeck	Variations in Value Orientations	1354
Clyde Kluckhohn	Values and Value Orientations in the Theory of Action	680
House et. al	Culture, Leadership, and Organizations	497

Table 6.1. Comparison of Citations based on Google Scholar

Fig. 6.1. Search Hit Comparison: Cultural Models (Google Scholar)

both crucial to our topic. Focussing on Hofstede's and Hall's cultural dimensions does not cover the entire spectrum of cultural characteristics and does not exhaustively address all cultural characteristics that might have an influence on information security. However, for reaching the goals of this thesis, this is not necessary and probably not even possible. Since hardly any research has been conducted on the edge between cultural studies and information security, any choice of characteristics might seem rather arbitrary. Working with Hofstede's and Hall's dimensions, which have been reviewed, critiqued and replicated for decades, is the most logical choice to start research in this field. In this chapter, I will therefore focus on Hofstede's and Hall's cultural dimensions. I will not go through them in their chronological order – Hall developed his dimensions before Hofstede – because I would like to focus on cultural

characteristics of one culture first and afterwards expand our view to the interaction between individuals with different cultural backgrounds. Of course, interaction with others (clients, colleagues, superiors, etc.) will also play a pivotal role when analyzing Hofstede's dimensions. However, Hall explicitly focuses on this interaction and by discussing Hofstede's dimensions first, we can incorporate some of these findings in the discussion of Hall's dimensions.

6.1.5 Applicability of the Selected Dimensions

Since Hall's dimensions can be seen as a generic description of intercultural communication characteristics and do not quantify cultural characteristics on a scale, they have been discussed and built upon but hardly criticized.[19] Hofstede's dimensions, on the other hand, have been scrutinized and are the subject of various controversial discussions. I would like to give room to this discussion and briefly discuss the applicability of Hofstede's findings to Chinese culture.

Applicability of Hofstede's Model for Analyzing China

Hofstede's cultural characteristics have been discussed and criticized from many different perspectives. I would like to focus on the criticism which is most relevant for the topic of this thesis, the applicability of his dimensions to Chinese cultural characteristics. The main deficiencies of Hofstede's model for analyzing *Chinese culture* are the following:

- There is no such thing as *the Chinese culture*[20] but Hofstede's model only describes national cultures and does not allow multiculturalism.[21] Even if we focus on Chinese whose parents are both from the same regional and ethnic group, there might be other noticeable differences in their values. As I already mentioned, most values are acquired very early in our lives. The time of acquisition is extremely important. If we talk about Chinese, we not only have to differentiate between different ethnic, generation, gender, religious, etc. groups but also regarding regional differences. Individuals who grew up on the countryside have a set of values that largely differs from the one of people who were raised in cities like Beijing or Shanghai, or even abroad.[22] If we focus on Chinese who were born and raised in China,

---

[19] In order to be able to work with the characteristics of particular countries, I base my analysis on values of similar dimensions by other cultural researchers. If that is not possible, I analyze the impact of this dimension on an abstract level or show tendencies by providing examples.

[20] National cultures are very seldom in general. This is one of the main criticisms of Hofstede's research. See Baskerville (2003, p. 6 ff)

[21] See Slay, Darzanos, Quirchmayr, and Koronios (2003, p. 330)

[22] Chinese who were born abroad are sometimes called *Overseas Chinese*. They can have special names like *American Born Chinese*, depending on the country in which they were born.

there is another interesting group, Chinese returnees. The term *Chinese returnees* describes Chinese who were born in China, studied or worked abroad later in their life and afterwards came back to China again. These returnees share their values with many Chinese who never left the country. However, they might have different practices (symbols, heroes and rituals) because those are acquired later in life. It is therefore important to know the background of a company's and its service provider's employees in order to be able to anticipate potential culture-related security threats.

- Hofstede's questionnaire and his analytical methods were developed by Western researchers and might not be appropriate for analyzing non-western countries.[23]
- Hofstede only used five dimensions. These dimensions cannot cover all cultural characteristics. Hofstede's model might therefore be oversimplified for a modern cross-cultural environment.[24] Other researchers decided to establish models with a multiple of his dimensions.
- His survey results are not current enough. The Chinese culture underwent profound changes in the last century, especially during the past couple of decades. Values, which were manifested over centuries, might not have experienced as dramatic changes as practices. However, the Cultural Revolution (with diametrically different values than those which the society was based on before) and the rapid change from planned economy to free market economy certainly affected the view on those values and the behavior of Chinese people.[25,26]

Besides this criticism, Hofstede's dimensions are accepted worldwide as a highly valuable tool to compare cultures because they are based on a high number of recipients and validated by various replication studies.[27] Adjusted with the empirical findings from the expert interviews I conducted in China, they can be used as a first insight into Chinese culture. Even though they exhibit minor deficiencies describing Chinese culture today, his dimensions provide a simple framework that can be used for developing an approach to link cultural studies and information security.

This thesis cannot fully discuss the research methods Hofstede applied or the validity of his results. It is a first step to combine information security

---

[23] See Yeh (1988, p. 157)

[24] See Yeh (1988, p. 150)

[25] Erwin K. Scheuch studied the *attitude to work* in Germany over 30 years, which, during that period of time, differed by 30 percentage points. See Scheuch (1995, p. 60)

[26] See also Inglehart's theory of value shifts and Maslow's hierarchy of needs, described in section 5.5.7.

[27] Even though Hofstede's research shows certain deficiencies focusing on Chinese culture in particular, it is an excellent framework for highlighting differences and commonalities between Chinese, Indian, Japanese, U.S. American and German culture.

research with cultural studies. Hofstede's findings are used to explain the results of a survey conducted in China, which discovered various behavior-related security threats.

6.1.6 Country Comparison

While looking at different cultural dimensions, I will highlight the values and characteristics of five different countries: *China*, *India*, *Japan*, *the United States of America* and *Germany*

The comparison of these countries enables us to understand cultural differences leading to information security threats. Furthermore, comparing different cultural settings, we can analyze why certain security incidents occur in some countries but not in others. For comparing these countries, I incorporated a chart presenting all five countries and how they score on Hofstede's cultural dimensions.[28]

China

Since China is my main research object, I present the 'Chinese culture'[29] most thoroughly. Based on cultural dimensions, culture-related security threats are clustered and explained. Besides presenting how China scores on different dimensions and how this influences information security, I also briefly describe the historic development of cultural characteristics that turn out to be security-relevant.

India

India is still the country with the highest market share in business process and information technology outsourcing. India and China are in a fierce competition and a comparison of culture-related security threats can influence the selection of the outsourcing location. For understanding how Chinese culture affects information security, it is important to compare it to different cultures. Due to the outsourcing focus of this thesis, India is the most suitable choice.

Japan

Regarding Chinese outsourcing providers, a big share of their clients are companies based in Japan. Japanese firms value the proximity to China and many Chinese are able to speak Japanese. However, there are many intercultural conflicts between Japanese and Chinese which can be understood by examining cultural dimensions. These cultural clashes can turn into security threats.

---

[28] See figure 6.3

[29] I would like to state again that due to its enormous size, China (and the same is true for India and all other countries) is a mixture of many diverse cultures. There are various historical developments in China that happened simultaneously and influenced different geographical regions differently. During the rest of this thesis, I often generalize and abstract from the behavior of Chinese living in particular areas. However, whenever necessary, I highlight cultural differences within China.

United States of America

The USA are presented as an example of a Western culture.[30] Since most clients of outsourcing providers are US American firms so far, a comparison of Chinese and US American cultural dimensions offers valuable insights into potential intercultural clashes in the outsourcing market. In contrast to the comparison of China and India, the gap between Chinese and US American scores is enormous. Out of these cultural differences, security threats accrue.

Germany

German cultural characteristics are presented because Germany represents a 'European culture'. European firms have a growing demand for outsourcing services. Its presentation in this thesis is thereby of the same nature as the description of US American characteristics. Compared to Asian cultures and to the US American culture, German culture (and European cultures in general) can be seen as moderate.

The scores of these five countries will be presented for each of Hofstede's dimension.[31] China is the country I focus on. India is its fiercest outsourcing competitor. Japan is another Asian nation with a different cultural background and a major outsourcing client for Chinese firms. The USA are a large outsourcing market and a culturally rather 'extreme' country. Germany is an example of a European culture – ranking somewhere in the middle on most cultural dimension – and stands for Europe as another promising outsourcing market.

Hofstede's Model: Country comparison

In the following, I present Hofstede's country scores for the five countries I just introduced. The national cultural characteristics concerning Edward T. Hall's dimensions are not presented here but discussed in the respective section (see sections 6.6, 6.7, 6.8 and 6.9). I chose this approach because in contrast to Hofstede, Hall does not quantify his dimensions. An overview of all dimensions at the same time is therefore not feasible. The presentation of Hall's dimensions is closely linked to the explanations of particular security threats. I therefore decided to present the cultural characteristics of the five countries I focus on and explain their impact on information security at the same time. Therefore, this section is an overview and country comparison of Hofstede's dimensions.

---

[30] As we will see later, the United States can be seen as a rather extreme cultural setting. They score particularly high or low on many cultural dimensions.

[31] Later in this chapter, I will also describe how these countries can be categorized based on Hall's cultural characteristics.

Figure 6.2 shows Hofstede's scores for China, India and the United States. Figure 6.3 broadens the picture and further includes India and Germany. Table 6.2 lists the values that are visualized in figures 6.2 and 6.3. Hofstede's scores are presented here as an overview of the cultural characteristics of each country. The reasons for high or low scores on particular dimensions are explained later on.

Fig. 6.2. Comparison of Hofstede's Cultural Dimensions for China, India and the USA

	PDI	IDV	MAS	UAI	LTO
China	80	20	66	30	118
India	77	48	56	40	61
Japan	54	46	95	92	80
USA	40	91	62	46	29
Germany	35	67	66	65	31

Table 6.2. Country Scores: Hofstede's Cultural Dimensions

For scrutinizing how different the cultures of the selected countries are, I compiled a table (see table 6.3) with a score that is best described as *culture distance*. The culture distance describes the average value difference between the country scores of two countries. The higher a score, the larger the gap

Fig. 6.3. Comparison of Hofstede's Cultural Dimensions for Various Countries

between the cultures of two countries. The score for China and India is for example calculated as follows:

$$\frac{|PDI(China) - PDI(India)| + |IDV(China) - IDV(India)| + \dots}{5}$$

A score of 21.6 therefore means that, on average, the culture scores of China and India are 21.6 points apart. Table 6.3 lists the culture distances for all combinations of countries.

	China	India	Japan	USA	Germany
China	0	21.6	36.2	44	42.8
India	21.6	0	27	24.8	25.2
Japan	36.2	27	0	37.8	29
USA	44	24.8	37.8	0	10.8
Germany	42.8	25.2	29	10.8	0

Table 6.3. Culture Distance of Selected Countries

Examining Hofstede's cultural dimensions, there are a couple of evident characteristics that I would like to highlight. Looking at the big picture, comparing China and India to the other countries, their country scores seem largely similar. China and India have a culture distance of 21.6 compared to 44 and 42.8 if we compare China with the USA and Germany. The cultural difference between China and Japan also shows a larger gap (36.2). Even

though the culture distance between China and India seems small, it is still twice as large as the distance between the United States and Germany (10.8). This means that there are cultural differences between China and India that should not be neglected.

The culture gap between China and India, and even more between China and Japan, is surprising because many people talk about 'the Asians' or 'the Asian culture'. The gap shows that the Asian culture does not exist. In fact, the culture distance between China and Germany is not much larger than the one between China and Japan (42.8 compared to 36.2). Comparing China to the other countries listed above, taking culture distance as the only measure, it most closely resembles India, followed by Japan and Germany. The cultural differences between China and the United States are largest (culture distance of 44). This seems to correspond with the problems companies face adapting to the Chinese environment. Information security concepts and practices should be transferred to a country with a high culture distance without adapting to the new environment.

Regarding China and India, the main difference between their cultural characteristics can be found in the dimensions *individualism* and *long-term orientation*. India scores significantly higher on individualism[32] and China on long-term orientation.[33,34] Furthermore, there are slight differences between their country scores on *masculinity* and *uncertainty avoidance*. China scores higher on masculinity and India on uncertainty avoidance.[35] Both countries score very similar on *power distance* (China = 80, India = 77).

Comparing China and the United States, the cultural differences are significantly larger than between China and India. Most obvious are the differences in power distance and individualism.[36] In the United States, the power distance between people is a lot smaller than in China and US citizens are more individualistic than Chinese. Concerning uncertainty avoidance, the relation is similar to the one between China and India, the U.S. resembling India.[37] Compared to China, where the entire society is extremely long-term oriented, US Americans show the opposite behavior.[38] There is hardly any difference between the reception of masculinity in both cultures.[39]

An interesting question is if there is any correlation between these cultural characteristics and the overall level of information security in a country. If so, it would be possible to rank all countries based on cultural characteristics

---

[32] IDV: China = 20, India = 48

[33] LTO: China = 118, India = 61

[34] Please note that there are a couple of problems with Hofstede's long-term orientation dimension. These problems are further described in section 6.5. This dimension is therefore only used carefully in this thesis.

[35] MAS: China = 66, India = 56; UAI: China = 30, India: 40

[36] PDI: China = 80, USA = 40; IDV: China = 20, USA = 91

[37] UAI: China = 30, USA = 65

[38] LTO: China = 118, USA = 29

[39] MAS: China = 66, USA = 62

and thereby derive an information security ranking of those countries. In the following, I would like to try a rough but educated guess.

If we assume that the United States provide a more secure environment than India and China,[40] and that it is riskier to outsource to China than to India, we could expect to have the following relations between Hofstede's dimensions and information security:[41]

A small power distance and a high degree of individualism could have a positive influence on information security. A low degree of uncertainty avoidance might lead to security problems. Masculinity does not provide us with any direct hints because China, India and the United States score similar on this dimension.[42] Long-term orientation should be excluded for now (see above and section 6.5).

This study will neither prove nor neglect this hypothesis. I analyze and explain the relation between Hofstede's dimensions and security problems in China. Since the focus lies on security threats in China, no general relation can be proven. However, the analysis provides further evidence for this general correlation. Scrutinizing this relationship is an interesting mission for further research.

6.1.7 Linking Cultural Characteristics with Security Threats

In the following sections, I map Hofstede's and Hall's cultural dimensions with security threats. The following explanations are based on security incidents that I found during qualitative expert interviews in China. I will thereby provide insights into the reasons behind differences in human behavior concerning information security. This analysis is certainly not exhaustive. It neither covers all security problems in Chinese firms nor all Chinese cultural values. Further research will create a more detailed picture of security risks that threaten the outsourcing of IT services in and to China. However, the following analysis does show that national culture has a strong influence on information security and explains the underlying reasons for many culture-based security threats.

6.2 Power Distance and Individualism

According to the hypothesis we developed above, a large power distance and low degree of individualism are the two main characteristics that have an

---

[40] See, for example, Deloitte (2006, p. 9)

[41] Please note that this hypothesis is not empirically substantiated. The causal connection is not proven. The statement is just a claim that seems logical. In the following, it needs to be scrutinized further. We will see if we can find empirical evidence that supports substantiates this claim.

[42] If there is any relationship to information security, a high masculinity could have a negative effect.

impact on information security in China. In the following, we will see if there is further evidence that supports this hypothesis.

It is important to note that both dimensions, power distance and individualism, are closely interlinked. Their relationship is inverse, to be precise.[43] Collectivist societies usually show a high degree of power distance. The less powerful members in those societies expect and accept that power distance is distributed unequally.[44] The opposite is the case in individualistic societies. Their less powerful members do not accept their role and strive to improve it, also by challenging the status quo and the power distance that is present. Ashleigh Merritt and Robert Helmreich, who analyze the human factor in aviation safety based on Hofstede's cultural dimensions, examine three combinations of power distance and individualism:[45,46] *Collectivism and High Power Distance*, *Individualism and Moderate Power Distance* and *Individualism and Low Power Distance.* Combinations like individualism and high power distance or collectivism and low power distance are not present in any society. Many cultural concepts are based on both cultural characteristics so that an analysis of each dimension individually would make it necessary to either choose which characteristic to attach those cultural concepts and related security threats to or to repeat those concepts and security threats in both sections. Furthermore, by analyzing both characteristics together, I can directly address the interrelations between them and thereby generate a more holistic picture. In the following, I will therefore analyze Hofstede's power distance and individualism dimensions in one section.

Figure 6.4 shows the links between power distance (PDI) and individualism (IDV) and relates both dimensions to elements of Chinese culture. The relations shown here are not exhaustive – PDI and IDV are interlinked with many more cultural concepts – but they provide a first impression how and why PDI and IDV are interlinked. The table is fully based on Hofstede's book *Cultures and Organizations – Software of the Mind* and the links can be found directly or indirectly distributed over the book.

The concepts that are colored in red are those present in China. If we look at IDV, for example, we see that Chinese national culture is mainly collectivist, which correspondents to a low value of individualism. In collectivist societies, the cultural concepts of face and harmony are highly important.[47] Another

---

[43] See Moores (2003, p. 212)

[44] See Merritt and Helmreich (1996, p. 7)

[45] See Merritt and Helmreich (1996, p. 13 ff.)

[46] Merritt and Helmreich replicate Hofstede's findings in the field of aviation safety. They show that US American pilots have a strong tendency towards high individualism and low power distance. Asian pilots, those from Taiwan and Hong Kong in particular (Merritt and Helmreich did not analyze the attitude of pilots from mainland China), show collectivist and high power distance attitudes and behavior. This correlates with Hofstede's findings (USA: PDI = 40, IDV = 91; China: PDI = 80, IDV = 20).

[47] A detailed description of those concepts is provided later in this chapter.

example for cultural concepts related to PDI and IDV is the difference between shame and guilt cultures. Shame is the apparent concept in China (colored in red). Interestingly, most collectivist societies possess shame cultures. Guilt cultures are often present in cultures with a high degree of individualism. Please note that shame culture vs. guilt culture and rule by law vs. rule of law[48] are special cases. For both cases, there are corresponding concepts on the other side of the spectrum. All other concepts are independent. They might have corresponding ones, but if they do, they are not listed here. Some concepts can be either categorized under low IDV or high PDI (since they are directly related). I listed them with the cultural dimension they seem more closely related to.

China:

low IDV (collectivism)		high IDV (individualism)
● shame culture	⟷	● guilt culture
● guanxi		● personal opinion
● face		● privacy
● harmony		● creativity
● patriotism		● problem solving

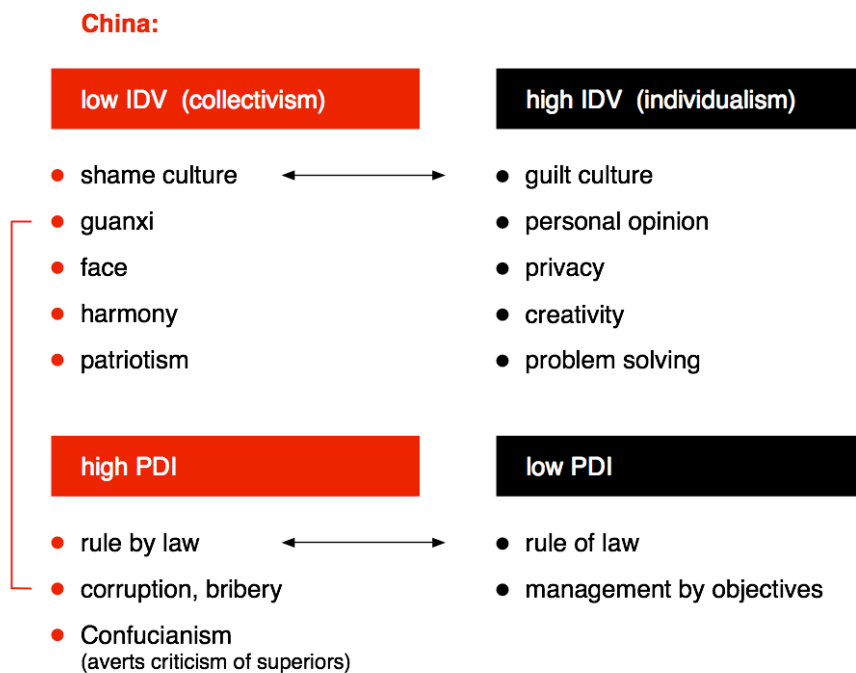| high PDI		low PDI
● rule by law	⟷	● rule of law
● corruption, bribery		● management by objectives
● Confucianism (averts criticism of superiors)		

Fig. 6.4. Linking Chinese Cultural Concepts with IDV and PDI

---

[48] Rule by law and rule of law are not cultural but legal concepts. However, they are directly related to cultural aspects and will be used later on so that they are linked with the respective cultural characteristics here.

6.2.1 Confucian Thinking – The Root of High Power Distance

About 2,500 years ago, Confucius (probably one of the best-known and most influential philosophers) lived in China, mainly in the province today known as Shandong. He developed a theory which he called wúlùn — five ethics or five cardinal relations. These relationships always define one group that is superior to another: parent and child, ruler and subject, husband and wife, old and young generation and friends (senior/junior).[49] According to Confucian belief, stability of a society is only possible if there is a high degree of inequality (which is the same as a large power distance). It needs to be clear who is superior and people have to act based on that principle. Mao Zedong was one of the very few Chinese leaders who seriously discredited Confucianism[50] – the rule of the proletariat did not need religions or social philosophies. At the same time, his own rules contained strong Confucian elements. His unquestionable power (a power distance as high as reached by the emperors in former centuries) is just one example. Confucianism has been the dominating philosophy for almost 2,500 years and is therefore deeply rooted in the Chinese mindset. Therefore, Confucianism can be seen as the root of high power distance in China.[51]

6.2.2 High Power Distance – China's Vulnerability to Social Engineering

Regarding information security, Confucian thinking – leading to high power distance – results in risks due to inadequate behavior of employees. Similar problems can be found in air traffic settings. I will first briefly address the impact of high power distance on air traffic safety and afterwards describe the relation between power distance and information security in detail.

Air Traffic Safety

In the field of aviation safety, it is fairly known that a high degree of power distance can account for safety risks. By conducting a survey among people working in the aviation industry (pilots and other crew members), Merritt found the following attitude to be related to a high degree of power distance: *Subordinates are often afraid to disagree with their superiors.*, *In abnormal situations, crew members rely on their superiors to tell them what to do.*, *Crew members shouldn't question the captain unless the safety of the flight is threatened.*, *Under no circumstances should the first officer assume command*

---

[49] See Ruey (1967)

[50] See Spence (1991)

[51] There are certainly many more reasons for the high power distance in China but Confucianism, and also Mao Zedong's leadership, have certainly shaped the society.

of the aircraft, etc.[52] Humans make mistakes and those mistakes can hardly be circumvented by technology. In a field where human error can be fatal, it is obvious that purely submissive behavior – no questioning of decisions and acts of superiors – can have lethal consequences. When a pilot makes an obviously wrong decision or acts illogically and the first officer does not take over the command, this creates a safety risk threatening the safety of the entire airplane. Even though the consequences in the field of information security might not be lethal, the same kind of problems occur. In the following, I would like to present examples which I discovered by conducting problem-centered interviews in China.

Information Security

Due to a high power distance, which is equivalent to steep hierarchies, Chinese employees are especially vulnerable to a form of attack called *social engineering*. For decades, the focus of information security efforts in companies was directed towards technical measures. Only in the last decade, companies became aware of the risk posed not by technical vulnerabilities but by inadequate behavior of their employees. Social engineering, the art of deception, can be traced back to the beginning of mankind. Tricking people into doing something that allows someone else to achieve his or her own goals is nothing new. However, companies only recently started realizing and taking countermeasures (like security awareness campaigns) against this form of attack. Social engineering is still widely used and probably the most promising attack on corporate information systems. Kevin Mitnick, presumably the best-known hacker in the United States, testified before congress in 2000 and revealed that he *"was so successful in that line of attack that [he] rarely had to go toward a technical attack"*.[53] Social engineering is based on insiders helping the intruder unintentionally. In high power distance societies social engineering is easy to conduct because the position in hierarchy (the rank) is extremely important. *"Rank [...] has its privileges, in particular the privilege of not being challenged by people of lower rank."*[54] Employees do not openly disagree with their superiors or other people possessing a higher rank than their own. This behavior leads to various security risks.

   Five interviewees, all outsourcing IT services to data centers in China, told me independently that they were extremely unsatisfied and sometimes even deeply surprised by the low level of physical security of their data centers.[55] When they wanted to enter their data centers, their background and thereby their authorization to enter the site was hardly questioned. Any form

---

[52] See Merritt (1998, p. 3)
[53] See Committee on Governmental Affairs (2000, p. 9)
[54] See Mitnick and Simon (2002, p. 52)
[55] Those interviewees outsourced to five different data centers, two of them even operated by US American firms (with Chinese employees).

of written legitimation was often accepted, no proper ID card was necessary. One company conducted a penetration test to find out how easy it was to enter their provider's site. They employed a consultant who printed out a business card with the name of one of their external auditors. The consultant faked an e-mail to the provider, pretended to be the security manager of the outsourcing client and told the outsourcing provider that the auditor had to physically check their servers. When the consultant arrived at the site, he only showed his self-printed business card and went straight into the data center. No questions were asked. The outsourcing client was not called back for verification and the security guard did not ask for a an unforgeable ID card. After entering the site, he was accompanied by a security guard which he told that he needs to work for a while and that he prefers working alone. The security guard left and the consultant could get access to any server in the building, not only the servers which belong to the company he had his mandate from. Another interviewee told me how he asked an intern to pick up a server from their data center and bring it back to their office. It had been down for a couple of hours and was not reachable anymore. He sent a fax to the outsourcing provider authorizing the intern to fetch the server. When the intern arrived at the site, he was not asked by anyone what company he was working for. He only told the guards that he was authorized by fax to pick up the hardware. When he came back to the office with the server, his manager was shocked. Accidentally, the intern had picked up the wrong server, not even belonging to the same company. He also had full access to other clients' hardware. When addressing the issues with the provider, it was even revealed that the provider never received a fax authorizing the intern to enter the building and to collect the server because the manager had sent it to the wrong number. Therefore, not only had the intern gained access to another company's hardware, even before, he managed to enter the data center without any legitimation and without being questioned. These security problems seem to have a cultural explanation which I will present in the following. The reasons are deeply rooted in the cultural background of the security guards.

Based on many talks with the outsourcing providers and their security guards, it turned out that they knew the rules how to check people arriving at the site. However, they were overwhelmed by the situation. The security personnel, who was in charge of the physical security of the site, did not stop the people arriving at the site primarily because they were foreigners. As such, they have more power and should not be questioned. Since one of the 'attackers' was trying to circumvent the security and the other one was sure that his superior had authorized his visit, both showed a very confident behavior and did not leave any doubt that they were allowed to enter the site. The security guards were simply afraid of scrutinizing their backgrounds because they did not want to question the foreigners' authority. Since foreigners are considered as superior, they cannot possibly be questioned. The same situation could have occurred with Chinese intruders instead of foreigners as well because those would also have a higher social status than the guards. However, it is

likely that they would have received a more profound scrutiny. The security risk of foreigners entering the site without authorization is also larger due to other cultural characteristics – the language barrier and the concept of face.

6.2.3 Language and the Concept of Face

The concept of face, as it is perceived in China, refers to two distinct Chinese words and concepts: mianzi and lian.[56] Mianzi refers to prestige (a high social status), as it is also known in Western societies. Lian, on the other hand, represents the moral integrity of a person.[57] Lian also stands for *"dignity, self-respect, feeling of social concern and ability to fill social obligations in front of other people"*.[58] A loss of mianzi undermines a person's social standing (or authority) whereas a loss of lian results in a disrupted relationship due to a loss of trust. When we talk about face, mianzi is the concept that is most often referred to. Not being able to speak English means a loss of face, mianzi, for security personnel because the social status appears to be lower than perceived before. But also lian, the morally correct behavior (sticking to social norms), plays a role in the course of this thesis.

Face is particularly important in collectivist societies. It does not only account for an individual but rather affects entire groups of people, like families, local communities, co-workers, etc. *"An employee's error may cause the company to lose face."*[59] Parents lose face if their children misbehave. Also the opposite is true. If someone gains honor, it is transferred to the entire local community or even the entire country.[60] The concept of face is not limited to China. It is also present in many other Asian countries and in Arabic and African societies like the Akan society in Ghana.[61]

While going through each cultural dimensions, I will frequently refer to the concept of face because it is omnipresent in the Chinese society and linked to many cultural characteristics. I present it here in detail because face is most closely related to collectivism (low individualism).

Air Traffic Safety

In section 6.1.3 I already presented examples of how language barriers and the concept of face play an important role in the field of air traffic safety. A pilot who does not understand the radio communication with air traffic controllers might have the feeling of losing face and thereby does not ask to clarify. This can lead to miscommunication and fatal accidents.

[56] See, for example, Ho (1976). For the relation between the concept of face and Hofstede's cultural dimensions, see Dong and Lee (2007).

[57] See Ho (1976, p. 867 f.)

[58] See Bedford (2004, p. 36) and Bedford and Hwang (2003)

[59] See Dong and Lee (2007, p. 405)

[60] The concept of face is closely related to national pride. The success of the Chinese Olympic athletes gave face to the entire country.

[61] See, for example, Agyekum (2004) or Obeng (1999)

Information Security

The language barrier and the fear of 'losing face' are two other important reasons behind the problems with the Chinese security guards described above. Imagine a foreigner trying to circumvent the security perimeter of a data center. Most security guards do not speak English and therefore do not know how to communicate with foreigners.[62] They are afraid to talk to foreigners because that would reveal their inability to speak English.[63] Since English is taught at school, every Chinese should have at least a basic understanding of the language. Not being able to communicate in English is embarrassing for many Chinese. They feel that they lose their *face*.

A similar problem inside the firm is also related to the concept of face. An interviewee who works for an outsourcing provider told me that if junior employees notice security breaches, they do not tell their bosses because it would be criticizing their decisions. Their superiors would lose face by making wrong decisions and putting the confidentiality, integrity or availability of company or customer data at risk. Another reason for not reporting the security breach is that it could only happen due to a mistake on the operational level. The employee who noticed the problem might himself be responsible for it. In that case, he will also not report it because he is afraid of losing face. My interviewee found out that in more than one case employees even wiped tracks of security breaches in order to cover their own mistakes. This makes later forensics impossible.

As I mentioned earlier, social engineering attacks based on high power distance and the concept of face are not restricted to foreigners. If the attacker is a Chinese employee of a higher rank, it can work the same way. However, foreigner intruders are likely to face an even lower hurdle than their Chinese counterparts because of the larger differences in hierarchy (high power distance) and the language barrier. Those factors combined are responsible for the fear of security personnel to lose face. Due to these Chinese cultural characteristics, in the examples I described above, intruders could enter data centers and leave the buildings with data and hardware without being questioned. Inside the firm, employees were unable to criticize mistakes of their superiors and felt the urge to hide their own mistakes. These incidents are only two examples that show how the concept of face can pose security risks.

---

[62] The same is true for a large share of Chinese security personnel in general, even though their employers try to convince potential clients of the contrary.

[63] Foreigners are not expected to speak Mandarin in China, even though they might have lived there for decades and might be fluent in the language. It is common that Chinese either reply in English or tell foreigners that they do not understand English, even if the foreigner addressed them in perfect Mandarin. The expectation to hear another language makes it sometimes impossible to recognize the own.

6.2.4 Individual versus Collective Efforts

High power distance societies often show tendencies towards collectivism (as opposed to individualism). However, in business settings the importance of hierarchy often suppresses the collective effort. Within corporations, group members always know who the leader is. They expect and even demand leadership from him or her. The decisions of the leader are hardly questioned which can lead to air traffic safety and information security risks.

Air Traffic Satefy

In collectivist and high power distance air traffic settings *"[g]ood communication and crew coordination are perceived as important. This is achieved via preflight briefings, the verbalization of plans, and the captain's coordination of cockpit and cabin crew."*[64] The pilot is the one who prepares the plan and communicates it to the rest of the crew. This plan is unlikely to be questioned since all other crew members have a lower social status. This kind of behavior is partially due to specifics of the air traffic environment. Even in individualistic and moderate power distance settings, the captain encourages questions from crew member but *"crew members should not question the captain's actions"*.[65] In Asia, flight attendants and pilots both prefer an autocratic captain who takes charge, especially in nonstandard situations.[66] Only low power distance environments acknowledge that the pilot might mistakes and not perform as necessary (e.g. due to fatigue). If the captain is seen as the unquestionable leader, flaws in his plans stay unrevealed and his mistakes in flight preparation as well as during the flight can have lethal consequences.

Information Security

Similar problems occur in the field of information security. Chinese cannot criticize decisions and behavior of their senior colleagues. In China, security concepts are often designed by one person instead a team of experts. Many of my interviewees described security concepts rather as rules that are set by management instead of a collective effort. The situation is similar in many Western countries. Security managers often develop concepts and set security policies without much interaction with colleagues and users. However, this practice happens to a larger extent in China and other high power distance countries.

In both fields, information security and air traffic safety, the absolute subordination creates security and safety risks. If a security manager does not

---

[64] See Merritt and Helmreich (1996, p. 13 f.)
[65] See Merritt and Helmreich (1996, p. 14 f.)
[66] See Merritt and Helmreich (1996, p. 18)

notice certain security risks or misevaluates them, they might not be properly addressed in the security concept. His subordinates (or even users) are unlikely to question the concept and suggest changes. A more collaborative environment would lead to a minimization of risks in both settings.

Similarly, a more individualist and low power distance environment, in which it is acknowledged that personal problems can affect the performance of all employees (even of high ranking managers), would also lead to a more secure (or safer) environment. Decisions made by superiors should be respected but security concepts should represent a collaborative effort. The fear of making mistakes and being punished for those mistakes should be minimized. Internalizing those principles into the corporate culture and exemplifying them through the behavior of managers can attenuate the risks that result from China's high power distance and collectivist (fear of loosing face) culture.

6.2.5 A Long Decision Making Process – The Fear of Decision Making

In China, this power distance relationship and the resulting risks are even worsened by a low sense of creativity and critical thinking. This is often apparent in collectivist societies. Predefined processes are followed precisely.[67] An independent working style, as it is supported in most Western countries, is often suppressed. Creative and critical thinking are characteristics that are not taught in Chinese schools. Teaching in high schools but also universities tends to be rather frontal. Of course, these education methods have an influence on behavior in the work environment.

Air Traffic Safety

In the field of air traffic safety, Merritt found that it is *"important [for employees] to know everything about the job, to have no surprises"*. Roles and responsibilities define how to react in which situation.[68] Strictly sticking to safety procedures is highly important to ensure safety and security. However, employees also need to be able to find creative solutions to unknown threats. In air traffic safety and information security, the variety of potential threats is unlimited. Ensuring a short timeframe between the identification of a problem and the actual decision of how to react is often crucial.[69] If there is no time to delegate decision making, employees need to be able to come up with

---

[67] There are also cases in China in which the opposite is the case. It depends on the working situation what kind of behavior is dominant. Concerning quality, rules and standards are often disregarded but a series of process steps is mostly followed. The lack of understanding of rules is explained together with the Chinese understanding of legal matters like contracts.

[68] See Merritt (1998, p. 3)

[69] One example of a situation in which fast decision making was crucial is the landing of US Airways Flight 1549 in the Hudson River on January 15th, 2009. Captain

a solution and execute it independently. Asian cultures hinder this form of problem resolution.

Information Security

Merritt's findings are also highly relevant for security settings. Thinking of uncommon attacks and protecting the systems by inventing and following creative approaches is rare in Chinese working environments. In case a security breach happens and there is no rule for how to react, the problem is normally not solved by the employees who notice it first. The decision of how to react is delegated to their superiors. A single employee does not want to take responsibility and is not used to solving problems on his own. The superior is often not able to react to the problem himself either and therefore does not take a decision without consulting with his boss before. This escalation of decision making results in a noticeable delay and can seriously harm the company.

Rule-oriented behavior and long decision making processes are also highly common in societies that tend to avoid uncertainty. I devoted an own section to critical thinking in uncertainty avoiding cultures.[70]

6.2.6 Relationships – Guanxi and Harmony

In collectivist and high power distance societies, especially in China, there is another concept which is almost as prominent as the concept of face. It is called *guanxi*.[71,72] Guanxi stands for a strong bond that can be formed by any kind of relationship. It can be the relationship with family members, friends, business partners, etc. Two people might have guanxi through commonalities even if they do not know each other. However, for a strong bond, there needs to be some kind of personal interaction in the past. This interaction can also be between the parents or other close relatives of two people, as it is often the case when two people grow up in the same village. Having visited the same school or worked for the same company also creates a bond. However, since guanxi can be seen as a relationship of trust, those relationships should rather be referred

---

Sullenberger only had very limited time to decide where to land and to prepare the emergency landing. If the decision making process had taken a little longer, the emergency would have turned into a disaster.

[70] See section 6.4, especially subsection 6.4.4

[71] See, for example, Xin and Pearce (1996)

[72] Yeung and Tung refer to a survey by Gordon C. Chu and Yanan Ju who interviewed 2,000 people in Shanghai about the importance of guanxi. *"92.4 percent affirmed the importance of guanxi in their daily lives [and] 71.7 percent preferred to use guanxi connections over normal bureaucratic channels to advance personal interests and solve problems."* See Yeung and Tung (1996, p. 58)

to as *relational demography*.[73] According to Jacobs (1976), two or more people might have guanxi if they share attributes, identity or origin.[74] However, for establishing strong guanxi, an interaction over a significant period of time should have happened.

Irene Yeung and Rosalie Tung analyze the concept of guanxi along six paths: *"the motives for engaging in social relations, reciprocation in social exchanges, time orientation, pattern of differentiation, nature of power, and sanction practice"*.[75] People in a relationship called guanxi normally fulfill a role that is based on Confucius' five cardinal relationships. Thereby, the relationship is not formed out of self-interest, as it is often the case in the Western concept of *networking*. According to Confucian ethics, people should strive to become a *righteous person*. Favors are being done when needed, but in return, the person who receives the favor is in a debt situation and should repay the favor. Guanxi can be imagined as a scale. It is not necessary to return a favor right away, directly after receiving one, but the scale needs to be balanced again in the future. This is another difference to Western networking. In the West, situations are often regarded as isolated events and the balance should therefore be equilibrate at any given time. In China, guanxi enables people to return favors after years or even decades – maybe even through family members. Favors are never forgotten but can be accumulated over time. However, in the end, they should be repaid with even larger favors. Harmony in the relationship is highly important. Helping disadvantaged can be regarded as a special case. Those might not pay back the favor themselves but the giver receives face for being a righteous person and helping out weaker people. Guanxi is so strong that it can overrule formal rules (like laws). Guanxi is based on ethics and is enforced by shame instead of guilt.[76] Losing face is the result of not giving or repaying a favor even though the guanxi would demand it. Summing up, guanxi can be seen as a relationship based on mutual trust. It is long-term oriented and no party normally pursues a direct goal. Favors are highly valued and repaid with even larger ones.

Air Traffic Safety

I could hardly find any studies in the field of air traffic safety that describe the impact of guanxi on safety management or that correlate guanxi with the likelihood of accidents. Hung-Sying Jing is one of the few researchers who tried to discover these relations. He describes the crash of a Taiwanese airplane 1995.[77] When the accident occured, the captain (who was monitoring), the first officer (who was flying the plane) and a stewardess were in the cockpit. Jing argues that the accident might have been prevented if the relations

---

[73] See Tsui and Farh (1997)

[74] See Jacobs (1976) as cited in Tsui and Farh (1997)

[75] See Yeung and Tung (1996, p. 55 ff.)

[76] For a deeper discussion of shame and guilt, see next paragraph.

[77] See Jing (2004)

between those three crew members would have been more loose. He argues that the pilot and the stewardess were chatting during the flight which might have distracted the captain. According to Jing, it would have been difficult for the captain to ask the stewardess to leave the cockpit (even if he had wanted her to leave) because this might have changed their relationship.[78] Even more fatal, the captain realized that something was wrong but did not stop the first officer from deviating from the route. This could also be attributed to the guanxi between the crew members. However, also Jing himself concedes that *"[m]ore evidence is required to prove that guanxi really influences flight safety"*.[79]

I assume that one of the reasons for the lack of studies on the relations between guanxi and air traffic accidents is the fact that crew members tend to change fairly often. If that is the case, a stronger influence on information security can be excepted. In the second field, work relationships last longer and there are normally more employees working as a group.

Information Security

Guanxi, the strong network of relationships, can lead to security problems in various ways. Interviewees told me that their companies employed people and made them in charge of information security even though they were not qualified for that job. This happened because those employees had good relations (guanxi) with managers in the firm. During my interviews, I found various cases in which it was hard for a company to fire IT staff that was either not capable of doing what it was supposed to do or misused their positions because they had good relations with high-level managers or were relatives of major clients and government officials. Furthermore, employees inside the firms helped outsiders to gain access, restrained from reporting security breaches, or even shared confidential data with people outside of the company, as a favor.

Another risk is posed on companies that outsource their IT operations — especially if they are foreign firms. Guanxi, which is very hard for foreigners to build up,[80] can pose a risk in legal disputes. Foreign firms face enormous obstacles if they would like to sue an employee, for example for breaking a non-disclosure agreement, a service provider (in the worst case a state-owned enterprise) for not sticking to the negotiated Service Level Agreement, or even the state.[81] Since the beginning of official trade with China, if a foreigner company sued a Chinese firm or employee it was unlikely to win the case.

---

[78] Jing argues that if a stranger had been in the cockpit, an extremely quiet cockpit could have been the result. See Jing (2004, p. 141)

[79] See Jing (2004, p. 142)

[80] Please remember that building up guanxi is a long-term process that requires a lot of trust.

[81] Please note that contracts with Chinese partners are still today very often a description of the status quo and not considered to be binding. There are numerous

Even nowadays, high-level executives are well-linked with courts and *giving or returning a favor* as well as real bribery is still fairly common.[82]

Guanxi can also have a positive impact on the relationship with the out-sourcing provider. If a strong relationship based on trust has been established and the provider feels treated well – maybe by not enforcing SLA penalties if one sees that the provider takes countermeasures for solving those problems in the future – it will do anything to maintain this harmonic relationship. However, establishing the relationship in the first place is hard for foreign companies that would like to outsource their IT services. The bond of the outsourcing provider with its employees and people outside of the firm is often stronger.

6.2.7 Shame and Guilt Cultures

The last cultural concepts that I would like to describe in this section is the concept of *shame and guilt cultures*.[83] It illustrates how social control is exerted in a society. Ruth Benedict describes the difference between shame and guilt cultures as follows:[84]

> True shame cultures rely on external sanctions for good behavior, not, as true guilt cultures do, on an internalized conviction of sin. Shame is a reaction to other people's criticism.

Both, shame and guilt, are possible forms of sanction. The main difference is that shame requires an audience – or at least the impression of an audience.[85] Guilt does not require any other person and can be evoked as a state of mind without any interactions with other members of society.

Shame is considered to be the dominating idea in many Asian countries (mostly collectivist). Western countries (individualist) tend to be more guilt-driven. The concept of having, giving and losing face is also directly linked with shame and therefore coincides with shame-driven societies.[86] Shame is felt by the family, or other people with close ties, as well as the person who makes a mistake himself. Therefore people try to avoid mistakes getting public not only

---

other problems with the Chinese legal system (a long history of rule by law and ethical rules instead of codified laws, insufficient education of lawyers and judges, etc.). Due to China's accession to the WTO this is slowly changing and China is stressing the rule of law. See section 4.3

[82] For further information on legal deficiencies in China, see section 4.3.

[83] In the West, a distinction between different kinds of shame of guilt is uncommon. In China, however, Olwen A. Bedford discovered three main types of guilt and four variations of shame, each having its own name. For more information see Bedford (2004, p. 32 ff.)

[84] See Benedict (2005, p. 223)

[85] See Benedict (2005, p. 223)

[86] See West-Newman (2006, p. 327 ff)

for protecting themselves but also for protecting their close relatives.[87] Guilt can only be felt by the person himself because is it directly linked to one's actions.[88] This explains the dominance of the concept of shame in collectivist and guilt in individualist societies.

Air Traffic Safety

"[I]n individualist cultures communication is made explicit and – in case of mistakes – people are guided by guilt that functions as private inner pilots, rather than shame that only evolves if a mistake has become known by others."[89] Individualistic cultures, resolving inner conflicts with guilt rather than shame, tend to suffer relatively less accidents.[90]

Information Security

Ruth Benedict relates guilt to the West and its criminal justice system.[91] As described in more detail in section 4.3, China does not have a long history of codified rules and laws. Rule of law is a new concept in China and the Chinese society slowly adapts to the new system but does not possess the necessary foundation in its cultural values. Security policies are normally codified like laws in order to be distributed within the organization and imposed on business partners. In Western countries, due to their guilt-driven morality, employees tend to stick to rules and therefore also to security policies. They feel guilty if they act against them. It does not matter if they get caught or not, they are supposed to feel guilty anyway. In China, on the other hand, employees try to stretch policies. Even if they intentionally disregard them, they do not feel as guilty as their Western counterparts.[92] It is not until they get caught by their superiors, or other people recognize their mistakes, that they start feeling ashamed because they lose face.[93,94] In consequence, security policies are less strictly followed in China than in Western, guilt-driven

---

[87] Merritt and Helmreich, based on Bond (1991), describe the relation between individuals and their relatives as follows: *"There is a motivating sense of shame not to disgrace the other group members with one's weakness or failure."* See Merritt and Helmreich (1996, p. 7)

[88] See Weiner (1996, p. 276 f.)

[89] See Soeters and Boer (2000, p. 118) based on Hofstede and Hofstede (2005)

[90] See Soeters and Boer (2000, p. 123)

[91] See Benedict (2005) or West-Newman (2006)

[92] For an analysis of what kind of circumstances evoke pride, guilt and shame in the United States and China, see Stipek (1998).

[93] As described above, the same problem can be observed in air traffic safety.

[94] But even when Chinese employees get caught many of them do not feel ashamed according to several of my interviewees. My interview partners often experienced that those employees tried to excuse themselves with phrases like buhaoyisi, which is a very common and weak expression of feeling embarrassed. Those employees went on working afterwards as if nothing had happened.

societies. Security managers cannot rely on them and need to observe their compliance frequently. This also means that in the field of information security, as it has been acknowledged for aviation safety, *"one size fits all training is inappropriate"*.[95] Transferring security policies without adapting them and their enforcement measures to local cultural characteristics is unlikely to lead to expected results.

6.2.8 Concluding Remarks

As we saw in the course of this section, Hofstede's cultural characteristics of power distance and individualism have a strong influence on information security in China and on information security in outsourcing relationships. Both dimensions are highly interlinked with traditional Chinese concepts that have been present for centuries and are unlikely to change in the near future.

Whereas high power distance has a negative impact on information security, a high degree of individualism reduces information security risks. In China, scoring high on power distance and low on individualism, various security threats arise out of those cultural characteristics. Masculinity and uncertainty avoidance also seem to influence information security in China as we will see in the next two sections. However, most culture-related security issues arise because of China's high power distance and its collectivist ideal.

6.3 Masculinity

Masculinity is mostly unrelated to Hofstede's other cultural dimensions.[96] Characteristic for masculine cultures is that challenges, earnings, recognition and advancement are important. Men are expected to be ambitious and tough.[97] Even boys should compete in class and try to excel. At the workplace, conflicts are being resolved *"by letting the strongest win"*.[98] Masculinity is a cultural characteristic that varies between countries, but also professions have a tendency towards masculine or feminine work cultures. In the air traffic industry, for example, *"the pilot image is traditionally portrayed as a solo enterprise of power and daring (man and machine). Individuals who are attracted to piloting are therefore likely to be more individualistic and more concerned with achievement and masculine style than perhaps individuals who are attracted to farming, teaching, or nursing as a profession."*[99]

If we look at the masculinity dimension (MAS) and compare our group of countries, there are a couple of aspects that should be noted:

---

[95] See Merritt (1998, p. 283)
[96] See Hofstede and Hofstede (2005, p. 122 ff.)
[97] See Hofstede and Hofstede (2005, p. 136)
[98] See Hofstede and Hofstede (2005, p. 147)
[99] See Merritt (2000, p. 299)

- The masculinity scores for all countries (except Japan) are rather similar (China = 66, India = 56, Japan = 95, United States = 62, Germany = 66). There are no large cultural differences concerning masculinity.
- The scores are no extremes. Except for Japan, all countries we analyze here score between 56 and 66. This means that the countries we focus on show neither extremely masculine nor feminine tendencies.
- Compared to the United States and India, China's culture seems to be slightly more masculine.

The impact of masculinity on information security is certainly more hidden than for power distance and individualism. China's moderate masculine tendencies made it difficult to observe security risks based on this dimension. However, there are a couple of security threats that could be identified and which seem to be based on China's slightly masculine society.

6.3.1 Competition – The Drive to Advance

One of the cultural characteristics that is based on masculinity and relevant for information security is the aspect of competition. In masculine societies, men are supposed to be tough and focused on material success, which leads to a high competition in companies and pressure from society. Since China, as well as India, the U.S. and Germany, scores slightly higher than average on masculinity, they show tendencies towards a competitive environment.[100]

Interestingly, due to China's strong collectivist culture and Confucian values, there is no direct, open competition. In Western companies, competition is more openly discussed and acknowledged than in Chinese firms. In the West, most people are aware of the fact that often two employees are running for the same position and those employees more or less openly distinguish themselves through hard work and obvious grouping with their supporters. Chinese employees rather compete 'behind the back' of others and try to gain power by secretly building up their team of supporters within the firm. If an employee believes that he will fail reaching his goal and many other employees already realized his ambitions, he is likely to leave the company without risking a direct loss against his competitor. Those intra-company conflicts might destroy the working environment and thereby create security risks. Most of my interviewees, especially those with foreign backgrounds, had difficulties understanding those team dynamics and had to rely on information from Chinese colleagues to understand their teams. Mending broken working relations was almost impossible for them and they were often told that they do not understand the problems because they do not understand the Chinese culture and the way social relationships work.

---

[100] As noted above, Japan is a special case. It is one of the most masculine countries in Hofstede's study.

6.3.2 Internal Conflicts Continued

Internal competition leads to problems concerning internal communication and interpersonal relationships within companies operating in China.[101] Individuals try to get around official rules and do things without sticking to official processes, even tricking their colleagues or superiors. If there is a security breach in a system that one employee administers, he might not report this incident to his superior and might not start executing the defined contingency plan because he is afraid of losing face. This loss of face might reduce his chances of being considered for promotions in the firm. In the worst case, this employee might even destroy systems or data, or disclose internal information and pretend that it was the fault of another employee, in order to protect his own face or to get rid of internal competition.[102] This situation is even worse if a high masculinity score coincides with large power distance, as it is the case in China.

Collaborative efforts to conceptualize and to implement security measures are less likely in high masculine societies because, as for high power distance, people try to protect their jobs by stressing their roles. A security manager develops the security concept and delegates it down to his subordinates for implementation. Thereby, the best result, which is normally the outcome of a team effort (people have different perspective and ideas), is not guaranteed in highly masculine environments.

6.3.3 High Turnover is Critical

Many of the problems due to masculinity can be explained by external pressure. In China, there is an enormous pressure, especially on men, to increase wealth and to step up the career ladder as fast as possible.[103] This pressure, amongst other factors, leads to a high turnover of employees. They tend to leave the company as soon as there are other, more promising options. Since China still has a lack of highly skilled personnel, those options arise as soon as one gained a little bit of working experience – especially if it is gained in foreign firms.

---

[101] Kjell Mjøs, analyzing the team function on the flight deck, also found that *"[h]igher scores on the PDI and MAS dimensions in [one of the companies he analyzed] may have negative effects on group process factors such as interpersonal relations and communication."* See Mjøs (2004, p. 166)

[102] Cases like the ones described are not theoretical considerations but happened in quite a few of the firms I interviewed.

[103] Buying an apartment for the own family very early in life, hosting an outstanding wedding party and various other social spending are important for the standing of the entire family. Those events define its social rank. Therefore, those obligations pose enormous pressure on young couples if their families cannot support them financially.

A leaving employee always poses a security threat on his former employer. Most interviewees, working for outsourcing providers, companies that outsource their IT services but also lawyers, all reported similar problems. They told me that many employees do not stick to non-disclosure agreements they signed with their employers. Due to deficiencies in the Chinese legal system[104] and the general problem of finding evidence for unsolicited behavior, this poses a large risk. One interviewee, the managing director of an IT consultancy, even told me that some of his employees never returned their laptops after leaving the company from one day to another. Corporate and customer data floating around, or even being sold to competitors, is a crucial security issue. If the company does not disable or delete the accounts of their former employees fast enough, especially if their parting is not based on mutual consent, those employee can use their credentials to disclose internal information (confidentiality), change data (integrity) or thwart the availability of their former employers' systems.

6.3.4 Concluding Remarks

All security issues mentioned above are typical problems I discovered during the interviews I conducted in China. Especially extremely high turnover rates worry outsourcing providers and their clients.[105] High turnover is critical not only from a direct security point of view but also from a knowledge management perspective. Companies need to train their employees and the employees need to understand their employers' IT systems. Today, employees often leave soon after they completed their training and gained some working experience. Therefore, knowledge needs to be transferred to successors. This is difficult to assure if people are bought out of the company from one day to another and leave without a proper transition period.

Masculinity seems to show some correlations with information security risks. However, the correlation is not as strong as for power distance and individualism. A high degree of masculinity has a slightly negative impact on information security because high competition leads to internal conflicts and high turnover. Out of those problems, security threats can arise. Since the influence is rather small and China scores moderately on masculinity, the impact of this dimension on information security while outsourcing within or to China is rather limited.

6.4 Uncertainty Avoidance

Uncertainty avoidance is the degree to which people tolerate ambiguity in life. People with a weak uncertainty avoidance do not need formal rules and

---

[104] See section 4.3

[105] Of course, the problems is not limited to companies working in the IT industry. High turnover is a general problem in China at present.

standardized processes. They are willing to resolve problems themselves and find ways to achieve their goals. There are some minor and rather indirect links between uncertainty avoidance and information security incidents that I observed in China. I will present those in the following.

6.4.1 Disrespect for Formal Rules

There is an *"emotional need for laws and rules in a strong uncertainty avoidance society"*, *"countries with weak uncertainty avoidance can show the opposite"*.[106] Considering a case from the aviation industry again: *"[T]he commercial aviation environment embraces high-UA behaviors such as checklists, manuals, and standard and emergency operating procedures as a way of managing error in a high-risk environment."*[107] China, which scores low on uncertainty avoidance, shows the opposite behavior. It has, for example, only very recently developed its legal system. In former times, the rule of man (or rule by law) and pure ethical norms, without codified regulations, were dominant.[108] Chinese never felt the need to establish formal rules because most situations could be resolved through personal interaction. Enforcing laws, and any other kind of regulation, opposes the doctrine of non-interference, called wúwéi, which is a dominant concept in Taoism. One interpretation of wúwéi is that the ruler should do nothing (inaction) to govern his country and that individuals do not need to force anything themselves either *"because it is the world (the Way [Tao] or the 'inevitable movement' of things) that is providing the motive force and carrying the Subject in the proper direction"*.[109] Another reason for this late transformation towards the rule of law is the high power distance in China. Laws were regarded as either unnecessary[110] or dictated by someone else anyway and not supporting the majority of the people.[111] In China, there is an ancient saying 'tiangao huangdiyuan', which literally means *the heaven is high, the emperor is far away.* It can be interpreted as *it is difficult to get justice* or as *being beyond the reach of the authorities.* The first interpretation expresses the Chinese belief that formal rules are not useful because they are difficult to enforce. The latter one suggests that sticking to the rules does not seem to be of high importance because it is unlikely that one

---

[106] See Hofstede and Hofstede (2005, p. 182)

[107] See Merritt (2000, p. 298)

[108] See section 4.3

[109] See Slingerland (2004)

[110] That is at least the case from a cultural point of view. Economically, many Chinese are aware of the fact that codified regulations are needed.

[111] Recently, partly due to China's accession to WTO, but also due to its growing economic exchange with other countries and their pressure on the Chinese administration, the legal system has started to develop according to Western concepts — not relying on ethical standards or dictated rules that come in handy for the leaders but laws that protect the people and their rights. For more information, please see section 4.3

gets caught or even punished for one's actions. Of course, the Chinese aversion against rules does not only exist towards laws but also other regulations like security policies. During my interviews, I hardly found any company that used and enforced well-defined security policies. If they had security policies in place, they were once created but never updated again. Employees often did not stick to those rules and they were not punished for disrespecting them. One company, that shortly before our interview received an ISO/IEC 27001 certification, established and tried to enforce strict security policies. However, they were understaffed. Without the necessary security personnel, even this firm could not properly enforce its rules.

6.4.2 High Turnover

In societies with low uncertainty avoidance, people are not afraid of losing their jobs or changing to a more promising one. According to Hofstede, *"in higher-UAI countries, other factors being equal, more employees and managers look for long-term employment"*.[112] This is for example the case in Japan which rates extremely high on uncertainty avoidance.[113] In China, the opposite is the case. Amongst other reasons (see above), China's low uncertainty avoidance motivates Chinese employees to change employers more often than people in other countries. This is especially the case in the IT industry where skilled personnel is scarce. As mentioned above, high turnover, resulting in a loss of knowledge and a higher risk of employees disclosing information about the company and its clients, poses serious threats to firms in China.

6.4.3 Nationalism

Chinese are well-known for their strong patriotism. The 1990-93 World Values Survey shows a relation between a low degree of uncertainty avoidance and the fact that people living in low UAI countries *"declared themselves more proud of their nationality and more willing to fight for their country than in strong uncertainty avoidance countries"*.[114] Even though there is no obvious link between nationalism and higher security risks, company representatives working in China told me that they are afraid of Chinese employees stealing internal information for the benefit of their competitors. This information could be sold or given away for free to private competitors or state-owned enterprise in order to support the development of the People's Republic.

---

[112] See Hofstede and Hofstede (2005, p. 182)

[113] Interestingly, employees in strong uncertainty avoiding countries tend to work harder than those who live in countries with a low UAI.

[114] See Hofstede and Hofstede (2005, p. 196)

6.4.4 Flexibility and Critical Thinking

As mentioned above, high uncertainty avoidance leads to a demand for clear rules and regulations. *"In countries with a low score for uncertainty avoidance, people have grown accustomed to solving problems independently; using improvisation; and, if necessary, acting outside formal rules."*[115] This is a rather general statement and this behavior could not be observed in China which might be due to its high degree of power distance. Whereas Chinese do act outside of regulations, creative problem solving and acting intuitively in unknown situation seems to be rather rare in China. On the contrary, interviewees told me of many incidents in which employees just sticked to the rules even though disobeying them would have been more appropriate. Many expatriates complain that Chinese employees need to be told what to do and do not show an independent working style. I assume this is also due to the Chinese education system, which is rather frontal. Those aspects do not seem to be captured by the uncertainty avoidance score that Hofstede derived for China. The influence of uncertainty avoidance on information security in China is therefore unclear.

6.4.5 Flexibility and Critical Thinking in Aviation Safety

To shine some more light on this dimension, I would like to compare outsourcing in China to the field of aviation safety again. Merritt states that crew members in uncertainty avoiding societies dislike surprises. They want clearly defined roles and responsibilities and are unable to react to unknown situations.[116] *"In (military) aviation, the precise following of rules is a matter of life and death. A large part of training (e.g., for pilots) focuses on learning to follow procedures and regulations. Previous training, extensive regulations, and flight preparation for all aspects of a prospective flight limit the risks as much as possible."*[117] Therefore, uncertainty avoiding employees, who stick to predefined rules, should have a positive influence on flight safety. Surprisingly, the opposite is the case. Since training situations cannot cover all potential problems that might occur during a flight, there are unknown situations in which pilots have to react intuitively, making their own decision. Soeters and Boer proclaim that in the 1960s Spanish trainee pilots had more problems reacting to emergencies than Danish pilots. The reason might be that Spain exhibits a stronger uncertainty avoidance. They therefore hypothesize that *"uncertainty avoidance and the occurrence of military aviation losses [...] correlate positively"*.[118] Pilots from uncertainty avoiding cultures get nervous during unknown situations, do not know how to react and therefore make mistakes.

---

[115] See Soeters and Boer (2000, p. 119)
[116] See Merritt (1998, p. 3)
[117] See Soeters and Boer (2000, p. 119)
[118] See Soeters and Boer (2000, p. 119) or Helmreich and Merritt (1998)

6.4.6 Concluding Remarks

Whereas the correlation between high uncertainty avoidance and aviation accidents can be explained and has been shown empirically by researchers in this field, the same conclusion cannot be drawn for the field of information security. The empirical data collected in China does not show this correlation. On the contrary, I found links between low uncertainty avoidance and behavior that might lead to security risks. However, this relation is only indirect and loosely. It might be the case that high uncertainty avoidance also leads to information security risks but since China has a low degree of uncertainty avoidance, this relation cannot be shown. Because I primarily focused on one cultural environment, I cannot say much about the opposite characteristic, high uncertainty avoidance. Furthermore, China is a special case concerning uncertainty avoidance because flexibility, which is normally apparent in low uncertainty avoiding societies, is suppressed by China's education system and its high degree of power distance. Since examples of both directions, positive and negative, can be found in China, the influence of uncertainty avoidance on information security should be rated with neutral for now. For a reliable assessment of the influence of uncertainty avoidance on information security, further research needs to be conducted in other societies, especially in those with a high degree of uncertainty avoidance.

6.5 Long-Term Orientation

There is one dimension in Hofstede's model that he derived scores for which are not opposed to but also not fully aligned with my findings. In Hofstede's survey, China scores extremely high on long-term orientation. In contrast, I came across many cases of short-term oriented employees. This is probably true due to the difference of long-term orientation in society and the behavior of individual employees. I mainly observed individual behavior and Hofstede's dimension are meant to describe values that underlie a society as a whole. Furthermore, focusing on highly skilled employees in the IT industry exhibits a bias. Compared to the rest of the Chinese population, those employees only represent a minority.

In order to explain the situation I observed in China, I would like to provide some anecdotal evidence. In November 2006, Janet Carmosky, a consultant who has been living and conducting business in China for over 20 years, gave a widely discussed talk on the China Forum in Chicago and defined the *Chinese mindset*.[119] Her findings are extremely simplified. However, they highlight tendencies in Chinese business behavior that are not aligned with Hofstede's findings. They rather support the results of my study. She

---

[119] Her statements are not scientifically founded but reflect the results that I derived from my interviews with IT security experts in China. It can be considered as another independent insight from the business perspective.

describes Chinese business behavior with the words *"Tomorrow never comes. When it does, you are free to start again like yesterday never happened."* or *"It is more important to be true to the opportunity than to some agreement you made previously."* Wilfried Vanhonacker, professor at Hong Kong University of Science and Technology, already came to the same conclusion in 1997: *"most Chinese companies seek profits on a much shorter time horizon than foreign investors"*[120] These statements underline the low uncertainty avoidance index (UAI) that Hofstede found but also contradict his high value for long-term orientation (LTO). They rather assign short-term oriented behavior to Chinese businessmen today.

6.5.1 Past versus Today and Rural Jobs versus Dynamic City Business

I believe that long-term orientation was very prominent in China for centuries but that this value dramatically changed in the last decades, especially after the Cultural Revolution (1966-1976). Long-term orientation might still be true for political changes implemented by the Chinese government. The Chinese administration slowly adapts to foreign standards, gradually opens its markets, shifts from a planned economy to a free market economy, and even begins allowing political participation and elections on a domestic level. This all is happening carefully, as a long-term transition. Five-year plans fix Chinese politics for a longer period of time and are still seen as short commitments. On the other hand, Chinese employees, especially highly educated, business oriented people who were born and live at China's Eastern coast, act more short-term oriented today. I assume that those changes in behavior were partly triggered by the hardship endured during the Cultural Revolution.

Some concepts Hofstede assigns to short-term orientation are very true for young Chinese today. A few examples, especially in the private life, are *"concern with social and status obligations"*, *"marriage is moral instead of pragmatic arrangement"* and *"living with in-laws is a source of trouble"*. Businesswise, some long-term oriented values are still present: *"investment in lifelong personal networks, guanxi"*, *"large savings quote"* and *"investment in real estate"* as well as *"leisure time is not important"*.[121]

Since it is unclear how young, well educated Chinese, who are the majority of people working in IT companies in cities like Beijing, Dalian and Shanghai, would score on the short-term versus long-term orientation scale, and because the findings of my survey partly oppose Hofstede's scores, I excluded this dimension from the analysis. I rather focused on Hofstede's four other values that correlate with the results of my study. Nevertheless, I would like to give a brief overview over long-term orientation and its potential impact on information security.

---

[120] See Vanhonacker (2004, p. 114)
[121] See Hofstede and Hofstede (2005, p. 207 .ff.)

6.5.2 Long-term Orientation in Business and Society

Concerning information security, long-term orientation should be split into two distinct dimensions. Whereas Chinese seem to be long-term oriented in private life and towards society (relationships play a pivotal role, family is highly important, etc.), especially young businessmen seem to be rather short-term oriented in their choice of and attitude towards their employer. This is exactly where problems arise. Since long-term relationships are often valued as more important than short-term business contacts, this gives room for bribery and unsolicited favors (like providing a close friend with confidential data). Employers are changed often by young high-potentials but friendships, or rather the entire Chinese relationship network (guanxi), is built and lasts for a lifetime. This difference in time orientation indirectly leads to information security problems. They are described in the chapter with the environmental factors[122] and as part of other dimensions.

6.5.3 Air Traffic Safety

Finding analogies to information security (with a focus on long-term orientation) in the field of air traffic is also difficult. Most studies exclude long-term orientation and rather focus on Hofstede's traditional four dimensions. In 2007, Wen-Chin Li and Don Harris published a paper named *Confucius in Western Cockpits: The Investigation of Long-Term Versus Short-Term Orientation Culture and Aviation Accidents.*[123] They try to show that long-term orientation causes air traffic accidents because it leads to negative organizational influences, unsafe supervision, preconditions of unsafe acts and unsafe acts of operators. For showing this relationship, they compare accident data from Taiwan with data from the United States. However, their reasoning does not explain why those safety issues are based on Taiwan's long-term orientation instead of Hofstede's four other dimensions on which Taiwan and the United States greatly differ as well. Due to the lack of solid research on long-term orientation and air traffic safety, broadening our view onto this field does not provide any further insights.

6.5.4 Concluding Remarks

As I mentioned above, I exclude the dimension of long-term orientation due to three reasons. First, my observations of Chinese business life are contradictory to Hofstede's scores which he derived for the Chinese attitude towards time. Second, long-term orientation only seems to have an indirect influence on information security. It correlates with many concepts that are described in other section of this thesis. Also a triangulation with the field of air traffic

---

[122] See chapter 4
[123] See Li and Harris (2007)

safety does not offer any further evidence on the relation between long-term orientation and safety (or security).

Before closing this section on long-term orientation, I would like to stress that in general, the business environment in China is still long-term oriented. Business cannot be conducted successfully without properly establishing a personal relationship between two companies that would like to pursue a deal. Foreign investors, but also clients that would like to outsource their IT services, are often extremely straight-forward in their way of approaching potential Chinese partners. Pressuring for decisions in the first meetings might ruin the relationship with the potential partner even before conducting any business. This behavior violates basic Chinese business rules and makes the Chinese company focus on short-term profits as well, instead of a long-lasting partnership, as it would be beneficial for any outsourcing deal. I will further analyze this problem in the following by focusing on Edward T. Hall's dimensions which provide insights into intercultural communication.

6.6 Context Orientation

Hall's dimension which he called *context orientation* describes how much information is coded into a message itself and how much is part of the context (primarily the relationship but also place, time, gestures, intentions, etc.). *"A high-context (HC) communication or message is one in which most of the information is either in the physical context or internalized in the person, while very little is in the coded, explicit, transmitted part of the message. A low-context (LC) communication is just the opposite; i.e., the mass of the information is vested in the explicit code."*[124] The differences between cultures are shown in how relationships are established, how communication is being conducted in general, how people deal with negotiations, the meaning of contracts, etc.[125] These differences in perception and communication make it hard for people with different cultural backgrounds to communicate, especially when one party comes from a low-context and the other from a high-context culture.

6.6.1 Country Comparison

For understanding different communication patterns, I would like to cluster the countries we focus on into high-context and low-context cultures. According to Hall and various researchers who built upon his model, most Western cultures tend to be low-context. Asian, Arabic and African cultures are mostly

---

[124] See Hall (1989a, p. 91)

[125] See, for example, Yum (1994) in Samovar and Porter (1994)

high-context. Context orientation loosely correlates with Hofstede's individualism dimension. Collectivist cultures can be regarded as high-context, individualist (and also uncertainty avoiding) societies tend to be low-context.[126]

Germany and the United States of America can therefore be clustered as low-context cultures. India, China and Japan belong to the group of high-context cultures.[127] But even within those two clusters, a differentiation based on the extent of context orientation can be made. India, China and Japan are not just all high-context cultures. China shows a higher degree of context orientation than India does. In Japan, even more information is coded into the context than in China. German communication is more explicit than it is the case in the United States. Figure 6.5 shows those differences and orders the countries we examine throughout this thesis based on their context orientation.
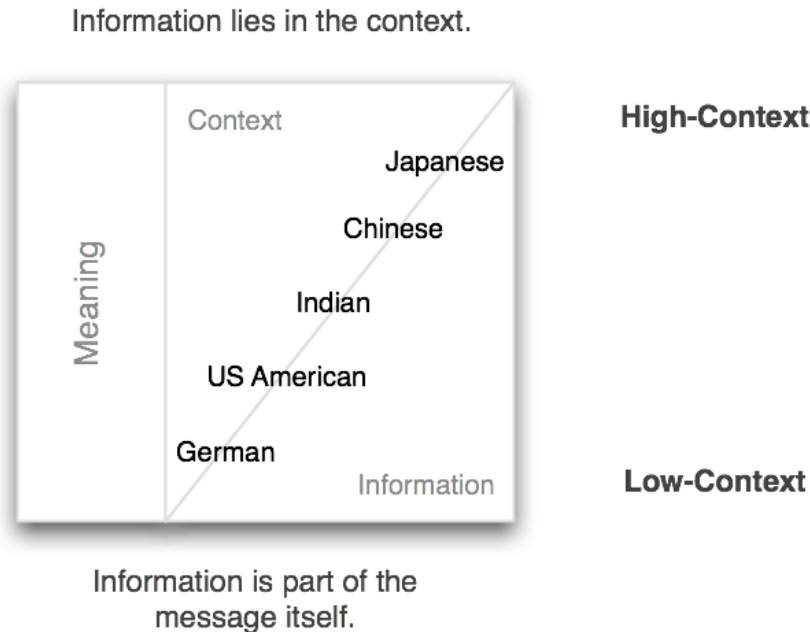
Information lies in the context.

Fig. 6.5. Country Comparison: Context Orientation

---

[126] See, for example, Hofstede and Hofstede (2005, p. 190 and p. 259) and Soeters and Boer (2000, p. 118)

[127] See, for example, Hall (1989a,b, 1994); Hofstede and Hofstede (2005); Kim, Pan, and Park (1998) and Lewis (2005)

The higher the difference in context orientation, the more likely there will be a communication problem between people from different countries. US Americans and Germans both belong to low-context cultures, Indians and Japanese have high-context backgrounds. However, US Americans and Indians are likely to have less communication problems than Germans and Japanese because their communication patterns are more aligned. The distance between high-context and low-context cultures is comparable to the culture distance that we defined based on Hofstede's dimensions. Unfortunately, Hall did not assign actual scores to each country but worked qualitatively. Therefore a score like communication distance between two countries cannot be calculated. However, it is important to keep in mind which cultures are more similar to the own one than others because communication risks and therefore also security risks increase with a widening gap in context orientation.

6.6.2 Establishing Relationships

Before writing about communication in different cultures, I would like to focus on how relationships are established. Relationships play a pivotal role in high-context cultures because a large part of information is hidden in the interpersonal relationship and not made explicit. Therefore, high-context cultures spend a lot of time establishing and maintaining relationships. Whereas US American tend to know many people and establish relationships very fast, Chinese and Japanese have a small network of people they trust. In the West, it is often easy to differentiate between friends and business contacts. In Eastern cultures, those two groups often overlap. Since a lot of time is spent on building and maintaining relationships with business partners in China, they become close friends. Furthermore, business is often conducted with friends because the trust relationship, which is necessary for doing business in China, is already established. This is also one of the reasons why friends or family members often work in Chinese businesses. Western managers look at hard facts like special qualifications. Their Asian counterparts value personal relationships because thereby they can blindly trust their colleagues and subordinates. The understanding of Chinese culture and its communication patterns, and even the relationship network of potential employees, should therefore play a major role in recruiting. *"The appointee should have in-depth knowledge of Chinese culture and the educational background to succeed in the characteristically indirect Chinese mode of communication in a high-context culture, and should be able to gain access to the relevant government bodies. For example, GM employed a key person who was fluent in Chinese, had strong connections with senior government officials and held the right educational qualifications."*[128] Since the relationship is highly important in high-context cultures, arguments and clashes, even leading to trials in front of courts, are

---

[128] See Liu and Roos (2006), based on Hall and Hall (1990b) and Graham and Lam (2003)

less likely. Everything is being tried to keep the relationship as harmonic as possible.

In the following, we will see how the relationship between two communication parties plays a pivotal role in communication, negotiation, contract management, etc.

6.6.3 Communication and Misunderstandings

The degree of context orientation of a culture can often be determined based on the characteristics of the language that is written or spoken in a country. The Chinese written language has changed very little in the past 3000 years. Some Chinese characters are pictograms or ideograms, most are ideogrammic or phono-semantic compounds. While Chinese characters are extremely hard to memorize and to decipher for new learners, by understanding the meaning of radicals, characters can be clustered and the meaning of a character can often be guessed out of context. Also the spoken Chinese language closely resembles the high-text orientation of China's culture. There are four tones in Mandarin Chinese and those tones determine the meaning of a word. However, even a word with the same tone can have different meanings. The meaning of a word can only be deciphered by the receiver of a message based on the context the sender creates.[129] The German language, on the other side of the spectrum, is extremely precise. Words with two different meanings are very seldom and the language itself exhibits redundancy to a great extent.[130] Reducing this redundancy for example by using all lower-case characters for writing, leaving out characters, changing their order or even switching the order of words, makes it harder but seldom impossible to read and understand a text. The necessity of context is therefore eliminated by redundancy in the language itself.

Context orientation can be observed on various levels. Languages themselves, written and spoken, can be high-context or low-context. But the way people communicate using those languages can follow either pattern. In high-context cultures, but also to a certain extent in low-context ones, understanding what someone really means depends on how it was said. The relationship

---

[129] Edward T. Hall states that written Chinese (in form of calligraphy) is considered to be art. He further proceeds that *"Good art is always high-context; bad art is low-context."* See Hall (1989a, p. 92) or Hall (1994, p. 63)

[130] I recently spent some time in Ghana. During my stay, many Germans but also US Americans complained about how imprecise many Ghanaians use the English language, especially when speaking pidgin English. However, the level of preciseness that many Westerners expect is often not necessary. Many African and Asian cultures are high-context and thereby a lot of information is coded into the context instead of the message itself. People with the same cultural background often do not have any problems understanding each other, even though outsiders, especially from low-context countries, cannot decipher the meaning of the conversation.

between communication partners plays a pivotal role in high-context cultures but without understanding the meaning of the rest of the context (place, tone of voice, gestures, past experiences, etc.) misunderstandings are likely. People from low-context cultures often ignore those signals which are part of high-context communication and thereby misinterpret high-context speakers. On the other hand, high-context receivers tend to misinterpret low-context senders because they pay attention to signals which are not meant to play a role in low-context communication patterns.[131] People from high-context cultures interpret more information into the message, see information that was not explicitly coded into it by reading between the lines and decipher the context. Reducing communication to purely work-related matters can be frustrating to them because they see social life as an integral part of understanding the other person and thereby the message he or she wants to send.
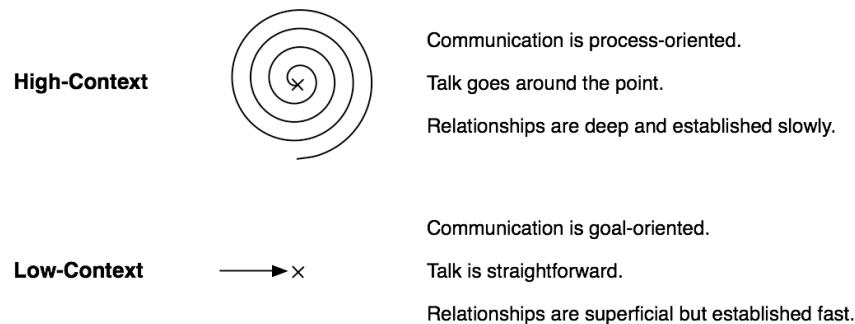

High-Context

Communication is process-oriented.

Talk goes around the point.

Relationships are deep and established slowly.

Low-Context

Communication is goal-oriented.

Talk is straightforward.

Relationships are superficial but established fast.

Fig. 6.6. Different Communication Patterns

The spiral in figure 6.6 represents the high-context way of building a relationship. It also shows how sensible topics are approached. To discuss important matters, a personal relationship needs to be built first. This takes time and required sharing of not only business but also personal information. As mentioned earlier, the relationship becomes an integral part of later communication. Furthermore, it must be maintained after being built up. This is one of the reasons why high-context cultures tend to have a small but extremely close group of people that can be called in-group members. This group normally consists of family, close friends and colleagues who are continuously being updated with news about what happens in one's life. The context is not created once but maintained continuously. Without this insider knowledge, it is hard to decipher messages and take part in a communication. Therefore, also low-context people should spend time building the relationship. They

---

[131] The communication patterns even within the group of high-context and low-context countries vary greatly. For a description of various communication patterns, see Lewis (2005).

should not focus on business right away (like in their home countries), as the second part of the figure shows.

The way topics are approached follows the same patterns as building a relationship. Germans and US Americans are goal oriented and shortly after opening the discussion address the issue they would like to talk about. Chinese rather lead to the issue by talking around it in the form of a spiral. Thereby, the issue at hand is often not clearly addressed at all. It becomes clear where the talk is heading while leading to the subject. By not addressing issues directly, nobody is put into an awkward position, or could even lose his face. The problem is addressed by reading between the lines and understanding the context. This form of communication can be observed in negotiations but also any other forms of discussion.

6.6.4 Yes, No and Maybe

Low-context communicators embarrass people from high-context countries by directly demanding something those cannot provide. In order to protect his face, a Chinese outsourcing provider is unlikely to say 'no' even if he cannot provide a requested service or security level. Saying 'yes' does not need to be an expression of agreement in high-context cultures. It can also be a form of protecting face and keeping the relationship as harmonious as possible.[132] This way of communicating can be highlighted by an example. An interviewee told me that he was talking with his outsourcing provider in the following manner: *"As you know, we found out in the penetration test last week that your employees' passwords do not comply with our security policies. Have you changed them?"* The reply was 'yes' but not a single password had been changed. In another case, a Chinese key account manager of an American outsourcing provider told me that he was approached by his major client a few months before our interview. The client told him: *"Our headquarter has changed policies and you need to be ISO/IEC 27001 certified within three months."* For the key account manager, that was an unreasonable deadline. If they wanted to get a certification at all, it would have taken more than a year to receive it. However, he told his client that they would comply. After two months, the boss of the key account manager, an American, found out about the conversation and called up the client. He told him that they had to cancel the entire contract. Receiving the certification was too expensive and not possible within the time frame demanded. In a personal talk between a manager from the client firm, the key account manager and his boss, it turned out that the client was happy with the service and also the security level the outsourcing provider had established even before requesting the certification. They wanted to stick with the provider and were shocked by them terminating

---

[132] Of course, answering with 'yes' even though the request is too high is not always purely related to protecting one's face. Potential providers can also agree on standards they cannot maintain in order to win a deal.

the service. What he meant to say was that it would be good if they received the certification as soon as possible so that the headquarter could not blame them if anything went wrong. The headquarter never asked for the certification, it was just a way of putting more weight into the negotiation. Without the context, the entire situation was unclear and could not be resolved until all information was shared.

A 'yes' does not necessarily mean yes in high-context cultures. Agreement can be a form of protecting face. It does not even need to be an intentional lie. Also, if situations or requests are unclear, yes or maybe are a common way of responding. There might be an action afterwards but the action might not fit to the request if the context is unclear.

6.6.5 Passwords and Privacy in the Office

After building a close relationship, there are hardly any secrets between members of the in-group. Sharing information is a way of building and maintaining trust. Privacy is less known in high-context cultures. Whereas Germans try to hide information about themselves, Chinese willingly share almost everything with their in-group. This leads to the discussion of salaries, which form an important part of the context and are therefore often discussed in China, but also the sharing of passwords. Since there are no secrets between close co-workers it is not necessary to keep a password secret. Many interviewees told me that it is extremely common almost everybody knows the passwords of everybody else in Chinese offices (if there are any passwords at all). Even the use of passwords makes people feel that there is a border between them. Protecting information is a way of expressing that there is a lack of trust. Sharing passwords is showing trust. If a Chinese is asked for his password and does not give it to a co-worker, this means that he does not trust him or has something to hide. This behavior can ruin the relationship and result in social sanctions. Therefore, passwords are freely passed around in the office. This makes it easy for an intruder to steal them. If he needs certain access rights, he can get them by asking the person with those rights directly or by finding out his or her password through co-workers. The more passwords people know, the more likely they are to write them down in order to remember them. Having unencrypted lists with login information of co-workers even on the desktop seems to be common in China.[133]

6.6.6 The Importance of Contracts

The understanding of contracts is extremely different in high-context and low-context cultures. Similar to their communication patterns, low-context

---

[133] Of course, post-its at the PC screen or under the keyboard are also common ways of remembering passwords.

cultures tend to produce long contracts trying to cover and codify every possible future development. In high-context cultures, taking China as an example, contracts are rather seen as a description of the status quo. They reflect the intentions of both parties at the time of writing.[134] The actual terms might even change until the contract is signed and are very likely not to be valid years after they were agreed upon. Contracts can be seen as a rough frame. However, this frame is not fixed. If assumptions of either side change during the partnership or if the partnership itself changes, the contract automatically changes as well. Many Westerners complain that it is unethical not to adhere to signed contracts. In fact, *"[i]n an American court of law, the attorneys, the judge, and the jury are compelled by custom and legal practice to pay attention only to what is legally part of the record"*.[135] However, Asians, mostly coming from high-context cultures, regard it as unethical to stick to a contract if the underlying assumptions have changed.[136] As I describe in more detail in the next paragraphs on long-term partnerships, the relationship is an essential part of contracts in Asia.

For Germans, even Scandinavian contracts and the way many companies deal with contracts is surprising. Understanding the role of contracts in high-context countries like China, but also in many other Asian, Arabic or African countries, is extremely difficult for them. US Americans, also having a rather low-context orientation, have similar problems.

6.6.7 Differences in Negotiations

Not only the contract itself has a different focus, also the way of getting there (negotiations) differs greatly in high-context and low-context cultures.

Low-context cultures like Germany, but also the United States, are goal oriented. Their goal is to reach an agreement and finalize it in written form. Westerners often reserve very limited time for talks with partners. They tell their potential providers for how long they will be in China – usually only a fraction of the time needed for negotiations in China – and expect their potential partners to free time according to their plans. Instead of building a relationship with their potential providers by collectively enjoying time in China (sightseeing, dinner, etc.) and getting to know each other, they bring their lawyers or consultants to the first meeting. This practice has a negative impact on the relationship right from the start. It shows the Chinese company that there is no trust and not even the willingness to build up this trust over a longer period of time. Lawyers are only needed in case of conflicts and those seem to be expected by the Western firm if they bring them even to the first meeting. In contrast to Western cultures, many Asian cultures are not goal

---

[134] Those intentions might not be part of the written contract. However, they are an essential part of the mutual agreement.

[135] See Hall (1989a, p. 89) or Hall (1994, p. 61)

[136] See Lewis (2005, p. 5 f.)

but process oriented.[137] The context is more important than the actual terms and conditions of the contract.

Let me underline the importance of the personal relationship, in negotiations but also afterwards, by presenting a short case. Two interviewees, who had been partnering with two Chinese companies for quite a while, told me independently that they had to find an excuse to decline the invitation of a partnering company to a brothel. Only after several meals, a visit to the opera and a Karaoke night, the relationship was mended and reached the same level it had had before the refusal.

The high-context approach of conducting business is not better or worse than the way things are done in low-context cultures. There are also advantages which Western cultures, focusing on short-term efficiency, often neglect. In a long-term relationship, there will be events outside of what has been expected before. Disputes are likely to arise at one point in time. Context-oriented cultures (similar to countries with a low uncertainty avoidance) know how to react to those unexpected situations. They solve them in amicable talks, both sides trying to find the best solution for both partners, instead resolving them based on legal ground.

6.6.8 Contract Management versus Mutual Partnerships Based on Trust

All guides to outsourcing mention that outsourcing partnerships must be managed. To be precise, they often refer to contract management. Even though the idea of not losing attention after the contract is signed and managing the partnership over the entire outsourcing period is correct, the focus must be adjusted. John D. Stees, for example, states in his book *Outsourcing Security – A Guide for Contracting Services* that is is important to *"[monitor] the contract to ensure that the selected provider adheres to the stipulations of the agreement and that the quality of service promised is produced"*.[138] Monitoring the performance by performing audits and inspections is a perfectly valid approach to outsourcing deals. Companies outsourcing in low-context or even middle-context countries are probably well advised to follow those guidelines. Even in high-context countries the importance of observing the performance of the outsourcing provider is obvious. However, it can only be part of the long-term efforts the outsourcing client puts in the outsourcing deal.

As mentioned earlier, in China, contracts are often seen as a rough guideline – an memorandum of understanding, portraying the intentions of both parties. However, more important, especially on the long run, is the partnership between the outsourcing client and its provider. The relationship does not only set a frame for the terms and conditions of the contract, it is the

---

[137] See Brahm (2004, p. 21)
[138] See Stees (1998, p. 77)

contract.[139] If a Chinese manager feels pressured in an unreasonable manner or if he feels that the client is observing his every step just to come in and sue him in case the services do not come up to the quality level defined in the contract, he will see the outsourcing relationship as a deal instead of a trust relationship. This might lead him into just performing up to predefined standards. Every additional request from the client will be billed or refused.[140] Some interviewees reported that their providers shut down and even sold their servers, which were used for hosting customer data, from one day to another because they felt that the relationship had been broken. If that is the case, confidential data might even be sold to outsiders for a quick profit. On the other hand, if the relationship with the provider is seen as a partnership and if the client shows generosity and support in case the provider has minor problems, this will build a strong relationship. Not enforcing every minor term of the contract and rather seeing the big picture will help building guanxi with managers of the outsourcing provider. In the end, they will work harder and even with a smaller short-term profit because they care about the relationship. Special requests will not be declined right away but the provider will try to do everything in its power to come up to the wishes of the partner.

As I said earlier, of course, the performance of the outsourcing provider should be monitored. However, building a personal relationship, maybe by having weekly meetings, exchanging employees and helping out each other, will build a long-term relationship beneficial for both sides. A harmonic relationship, based on generous judgement and behavior as well as positive thinking, is certainly better than resolving even minor issues in Chinese courts.

6.6.9 Security Awareness Campaigns and Security Trainings

The last relation between context orientation and information security is in the field of awareness raising and educating employees. Security awareness campaigns and security trainings that were developed in low-context countries should not be transferred to high-context countries without any adaptation. Very often, they are developed at the corporate headquarter or purchased from a Western security consultancy. To my knowledge, the Chinese security education market is just starting to develop and there is hardly any local security awareness material. This is problematic because the message has to be

---

[139] This expression is slightly exaggerated but it should stress the importance of the relationship in negotiating with Chinese and for maintaining a successful outsourcing partnership.

[140] Please note that this kind of behavior shows general tendencies based on traditional Chinese culture. That does not mean that there are no firms, especially those with mostly foreign management, which have adapted to Western working style. However, those problems (from the Western point of view) will persist for decades because cultural characteristics only change slowly.

delivered in a different manner.[141] Instead of purely educating employees, a personal relationship needs to be established. Employees need to feel part of the company and that it is a collective effort, even their social obligation, to maintain a high level of security. I believe that this approach should also be followed in low-context countries in addition to purely rational explanations. Some Western companies start making their awareness campaigns more personal and engaging. However, security trainings are still largely rule-oriented. They describe what can, should and should not be done, without providing the necessary context.

6.6.10 Concluding Remarks

Soeters and Boer expect low-context communication to have a positive influence on preventing and dealing with accidents in military aviation.[142] Low-context communication does not require to establish a relationship and does not rely on the interpretation of the context. The same judgement that they make for aviation safety might be true for information security but needs to be scrutinized further. However, there are also positive character traits of high-context cultures. For example, their urge to establish long-term partnerships. More important than judging the dimension itself is the awareness that a difference in context orientation is likely to lead to miscommunication and thereby to security problems. Before contacting potential outsourcing providers, the context orientation of the own and the target country should be examined. If there are significant differences, those should not be neglected and should be reacted upon.

6.7 Monochronic versus Polychronic Time

Monochronic cultures regard times as linear. It can be compartmentalized into different time slots and events are assigned to those slots. In polychronic cultures, on the other hand, many things can happen at the same time. Plans and deadlines change. The big picture (the context) is more important than minor details.

China is hard to categorize based on this scale. As Japan, it shows monochronic and polychronic characteristics. *"[...] in Japan the tightly scheduled monochronic pattern is applied to foreigners who are not well enough integrated into the Japanese system to be able to do things in a more leisurely manner, and where emphasis is on developing a good working relationship."*[143]

---

[141] Another important cultural characteristic that should be taken into account, concerning security awareness campaigns and trainings, is *preferred message speed*. See section 6.9

[142] See Soeters and Boer (2000, p. 118)

[143] See Hall (1989b, p. 58) or Hall and Hall (1990a, p. 114): *"The key to understanding Japanese time is to know that the Japanese have two modes: a monochronic mode*

The cultural characteristics in China are very similar. Time is valued and in order to make sure that other people's time is not wasted, Chinese usually arrive early at a meeting. However, the relationships to people are of higher importance than sticking to predefined plans. Richard D. Lewis has reacted to this deficiency by introducing a third type, cyclic time. His model, which I will use for the country comparison, is based on three different perceptions of time, linear (monochronic), multi-active (polychronic) and cyclic.[144]

6.7.1 Linear, Multi-active and Cyclic Time

The cultural types triangle (figure 6.7) presents Lewis' categorization of various countries based on his three main dimensions: Linear, Multi-active and Reactive. It describes general cultural characteristics of countries. By renaming reactive to cyclic, the diagram describes the way those national cultures deal with time. The diagram is not drawn up to scale and therefore the distance between the countries does not represent their difference in time orientation. However, they are ordered according to their cultural characteristics.

China and Japan can be regarded as countries with a cyclic perception and usage of time, Germany and the United States are linear-active and India lies somewhere between cyclic and multi-active. None of the countries we examine is truly multi-active. In Germany and the United States, time is highly precious. Those countries plan time in a linear manner, one event after another. Each event is assigned to a fixed time slot which should not be expanded or shifted. Multi-active cultures, like they are present in South American and Arabic countries, do many things at the same time (polychronic or synchronic) and their timetable is unpredictable.[145] Cyclic usage of time, as in China and Japan, lies in between those two extremes. They incorporate aspects from each perception and add their own perception of cyclic time. In their view, events reoccur periodically. Their perception is largely based on the observation of nature (rise and dawn of the sun, four different periodic seasons) and religion (e.g. Buddhism).

Chinese arrive at meetings even before Germans and highly value other people's time (linear-active perception). However, they also have a strong focus on building up a personal relationship and put the relationship before everything else (e.g. schedules and deadlines; multi-active perception). When discussing topics and trying to answer questions, they have their own way of dealing with time. They focus on a topic but do not cover it in every detail

---

for foreigners and technology and a polychronic mode for virtually everything else."

[144] Edward T. Hall describes polychronic cultures as having a cyclic perception of time. While it is true that they take into account the context, also recognizing the past and the future, his dichotomy falls short at describing Asian cultures. The polychronic paradigm rather fits to Mediterranean, South American and Arabic cultures, which Lewis would describe as multi-active.
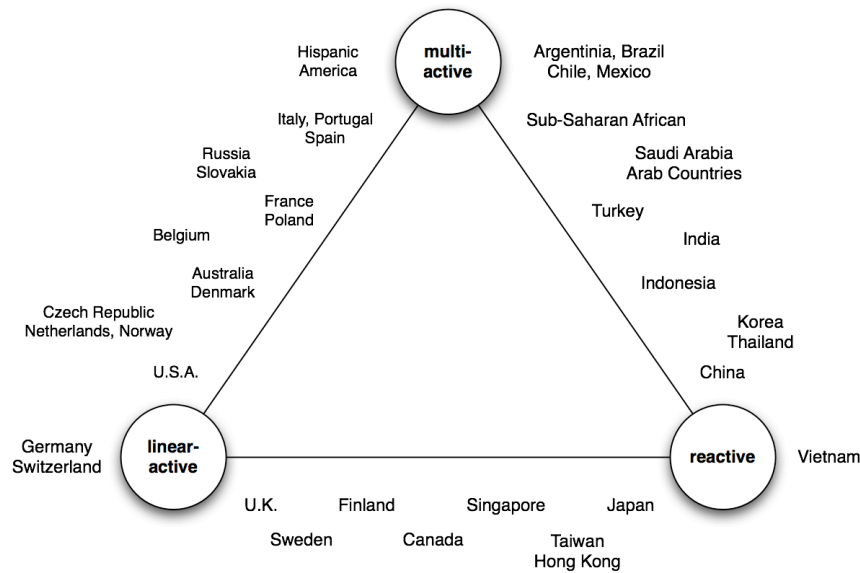
[145] See Lewis (2005, p. 33 f.)

Fig. 6.7. Cultural Types: Linear-active, multi-active, reactive variations

but rather discuss a variety of issues and later come back to the state where the topic was changed before (cyclic perception). This can be very frustrating for linear-active people in negotiations. When linear-active negotiators believe a final agreement was made, the topic can be raised again after a few hours by their Chinese counterparts without any negative intention.

6.7.2 Concluding Remarks

Lewis describes the following general relations between people from different cultures dealing with each other: The interaction between linear-active and multi-active people is highly difficult because their views are almost contrary. Interaction between people from cyclic and multi-active cultures is time-consuming but likely to lead to satisfying results. Cyclic and linear-active people get along well but have minor issues with cyclic people returning to formerly discussed issues and linear-active people devoting little time to the establishment of context, especially relationships.

It is likely that large differences in time orientation (monochronic versus polychronic or linear-active compared to multi-active and cyclic time) lead to minor information security problems. Communication is difficult, especially between linear-active and multi-active people, and multi-active people tend to disobey initial plans. This behavior is not expected by linear-active partners. However, since the countries we observe show similar and especially not highly conflicting characteristics (linear-active and cyclic communication part-

ners can cooperate rather well), I could not find any major security concerns directly related to the different perceptions of time. Negotiations and plans are handled differently but this difference was largely described in the previous section on context orientation. In further research, it would be interesting to analyze if problems occur when outsourcing from linear to multi-active environments and if more security risks can be found in multi-active cultures. For scientific purposes, focusing on Mediterranean, South American and Arabic countries would be most insightful because of their strong multi-active perception. However, analyzing Indian outsourcing deals would be most relevant because of its strong outsourcing industry and its hybrid culture, between multi-active and cyclic.

6.8 Space

Edward T. Hall introduced a theory about different concepts of measurable distances which he called *proxemics*. Based on spacing mechanisms in animal behavior (Which distance is critical and when should an animal flee?) he defined four distances that can be seen as bubbles surrounding our body:[146] *intimate distance*, *personal distance*, *social distance*, and *public distance*. Those distances define our behavior and what kind of distance is appropriate in which situation. Entering intimate distance without permission is considered as rude and even threatening. But also the invasion of personal space by a stranger can be highly inappropriate. Those spaces are defined by a variety of sensory inputs, ranging from visual and kinesthetic inputs to auditory, thermal and olfactory ones. The aggregation of those inputs defines the four distances. The perception of those distances varies from culture to culture. Proxemics not only play a role in personal distance but also in architecture, art, etc. Especially its influence on office layout and the perception of privacy plays an important role for the topic of this thesis. Before focusing on those aspects, I would like to show general tendencies of our countries towards the perception of space.

6.8.1 Country Comparison

In Germany, own private space plays a very important role, it even defines the status in society. The personal distance is large and an intrusion is considered rude. Even entering a space where one can see a private conversation, without possibly hearing it, is considered inappropriate. India, amongst the countries we examine here, seems to be the one with the shortest personal distance and the one in which privacy is least important. This is probably due to its regional and cultural similarity to Arabic countries, in which public space is

---

[146] See Hall (1990a, p. 113 ff.)

really considered public.[147] There is no privacy in public and the intensity of sensory inputs that Arabs feel comfortable with is overwhelming for people from most other cultures. The United States are closest to Germany in their perception of space. However, they value privacy less than Germans do. In the United States, people tend to stand closer to each other in social settings and private space, at least in the office, is less important. In Japan, due to its extreme population density, people have adapted and learned to cope with very little space. Homes are extremely small and public transport is often overcrowded (from a German point of view). Donald Keene even states that *"[t]here is, in fact, no Japanese word for privacy"*.[148] China seems to reside close to Japan and India. Privacy is not known in China and therefore nobody complains about intrusions. In China's traditional neighborhood alleys, called hutongs, people still often live – eat, chat, sleep, etc. – on the street. The entire social life takes place outside. Often, people have to live in their small shops, which means that strangers continuously enter their private space, their home. With the German perception of space, this would be intolerable.

6.8.2 Office Space

The largest influence of Hall's proxemics theory on information security is in the perception and usage of office space. Whereas Germans value their own office and shut their door behind them to have their privacy, the usage of office space is very different in other countries. In the United States, cubicles are very common. Office doors should stay open so that colleagues feel invited to raise questions and so that one can take part in social life. In India, Japan and China, especially in modern offices, open-plan offices are very common. It is common that they are not even divided into cubicles so that everybody works at the same space and can see everybody else. Even high-ranking managers often do not have an own office, which is also due to the urge to continuously provide and receive information – being in the center of the information flow.

In order to find relations between the usage of office space and information security, we can have a look at the *Baseline Protection Manual* by the German *Federal Office for Information Security*.[149] It devotes an entire module (Module 2.3: *Offices*) to the presentation of security threats related to an inappropriate use of office space and how to minimize those security risks. The Baseline Protection Manual describes threats resulting from a *lack of, or insufficient, rules*, *unauthorized admission to rooms requiring protection*, *impairment of IT usage on account of adverse working conditions* and human error like *hazards posed by cleaning staff or outside staff*.[150,151]

---

[147] See Hall (1990a, p. 154 f.)

[148] See Keene (1959, p. 16)

[149] See section 2.4.2 or the publication itself, BSI (2005)

[150] See BSI (2005, p. 95)

[151] Possible threats are of course not limited to those, but they give a first insight into how office structure can have an influence on information security.

For a company that makes use of open-plan offices, it is harder to protect the confidentiality of data than in a company that provides a lockable room for each employee. Furthermore, the risk of manipulation and theft of data is higher. In a large office without any walls, information on the screen or the desk of co-workers can be seen and telephone conversations overheard. If an employee leaves his desk, even only for a short period of time, he should lock his screen so that nobody can access his data. In the evening, when all other employees are gone, an employee who stays late, or even comes back to the office, can sneak through files of other employees. Hardware can be stolen easily by employees but also intruders who gain access to open-plan office. If most employees have own offices, they can lock their doors in the evening. In open-plan offices, all documents should be stored away in file cabinets (clear-desk policy) and hardware should be locked by using anti-theft devices.[152]

Physical and organizational measures should be employed to protect any office, but open-plan offices pose an even greater risk on the confidentiality, integrity and availability of corporate data. When I interviewed outsourcing providers in China, I often entered and left those offices, sometimes with a few hundred people working on the same floor, without any need for authorization at the entrance and without being escorted when leaving.[153] Spotting confidential information and also stealing laptop PCs, files and removable media would have been easy. This is true for private offices which were hardly protected as well but the risk is even higher in open-plan offices. For protecting the office space, the *Baseline Protection Manual* can be a useful guide. Doors with dummy knobs towards the corridor, locks with keys for authorized employees and a bell for visitors should be basic requirements for any office space. Additionally, organizational measures like a clear-desk policy, password-locked PC screen, escorting visitors, etc. are necessary.

There are two more special cultural attributes concerning office space that I would like to address: office space for the management and teleworking. In some cultures, high-ranking management is seated at the top floor or other prestigious spaces within the building. Other cultures rather have their management in the middle between their employees. One should be aware that the second seating rule might increase the risk of confidential information being disclosed. If managers sit in the same room as everyone else, their data is more easily accessible. In those setting, the management should receive a special training. Teleworking is also more common in some cultures than it is in others. If a culture supports teleworking, the respective security measures should be established in order to secure the working environment outside of the office building. This can be done by physical means but should also be accompanied with special awareness campaigns and security trainings for the teleworkers.

---

[152] See S 1.46 (use of anti-theft devices) and S 1.23 (locked doors) in BSI (2005)
[153] See S 2.17 in BSI (2005)

6.8.3 Privacy

I already slightly addressed but did not fully elaborate on the concept of privacy in the office. In cultures where privacy plays a less important role (China, India, Japan, etc.), the risk of unveiling confidential information is higher. Information can more easily be seen but also overheard on the telephone when working in open-plan offices. But also the American open door policy, in contrast to German offices in which the door is normally closed, adds to the likelihood of confidential information being revealed. If a culture does not have a strong sense of privacy, it is difficult to establish a feeling for the need of confidentiality. People might not lower their voice on the phone, as in cultures that focus on privacy. Thereby, confidential information could be overheard. They also tend to stay in the office instead of going to conference rooms for confidential conversations. This risk is reduced in China, compared to other cultures with a low sense of privacy, because Chinese employees try not to disturb their co-workers. However, the risk is still larger than in cultures like in Germany.

6.8.4 Concluding Remarks

There are many other cultural characteristics related to the usage of space (like the seating in meetings but also access for cleaning staff)[154] which can indirectly influence information security of outsourcing deals. However, the largest risk is related to the use of office space and the lack of privacy. The latter one makes it hard to establish a feeling for the need of confidentiality. The office and all data and devices in the office should be protected by physical and organizational security measures, adapted to the culture they are applied in.

6.9 Preferred Message Speed

Hall's last dimension is called *preferred message speed*. It describes the preference in speed in which people would like to encode and decode messages. Messages that are transferred fast usually consist of less information, or contain a less complex message, than slow messages. Examples for fast messages are headlines, cartoons and TV commercials. Slow messages are books, art

---

[154] I experienced many security incidents in Chinese data centers that occurred because cleaning staff was not properly educated and had access to confidential information. In one data center, servers were regularly down because one cleaning lady always unplugged the network connection because that made it easier for hear to clean the server room. In another data center, a server was stolen when a member of the normal cleaning staff was on vacation and replaced by a temporary worker. Problems with cleaning staff seem to be common. The *Baseline Protection Manual* explicitly addresses these problems. See T 3.6 in BSI (2005)

and TV documentaries. Besides those formats, message speed can also refer to relationships. If cultures prefer deep long-lasting relationships, they have a preference for slow message speed. Those societies in which a large number of contacts and a loose network of friends is important can be located at the other side of the fast-slow message speed spectrum.

6.9.1 Country Comparison

Preferred message speed shows similarities to context orientation. The United States, for example, are a low context society in which networking is extremely important. One needs to know many people and it is very easy to approach someone. Establishing close relationships is not as important as in many Asian countries. For keeping themselves up to date and for entertainment, US Americans also prefer fast communication channels. Television and cartoons are extremely popular. In many Asian countries, the opposite is the case. Deep relationships, guanxi in China, play a very important role. Newspapers,[155] poetry and art seem to be more popular than in the United States. By examining Europe, some differences to context orientation are revealed. In Germany, the country with the lowest context orientation, friendships and business relationships are established more slowly than in the United States. Poetry, newspapers, books, etc., all slow message speed formats, are more valued than in the United States. *"Buddha, Confucius, Shakespeare, Goethe, and Rembrandt all produced messages that human beings are still deciphering hundreds of years after the fact."*[156]

6.9.2 Learning and Relationships

There are two main relations to information security: the implementation of security awareness campaigns and trainings and the way relationships are built. Since I already wrote about the way relationships are established and how that has an impact on information security in detail,[157] I would like to focus on the way information security awareness campaigns and security trainings should be conceptualized and executed. Information security awareness campaigns and security trainings, the tools that educate employees, are highly important for establishing and sustaining a high level of information security. Like all other information, they should use the communication channel that is preferred by the cultures that is targeted. Releasing a cartoon or a short video to explain information security issues might not be appropriate in slow message speed cultures. Employees might find it too superficial and are unlikely to change their behavior because of the lack of context. On the other hand,

---

[155] In China, one can see many people standing on the street in front of glass cabinets reading the daily newspaper.

[156] See Hall and Hall (1990b, p. 5)

[157] See, for example, section 6.6

handing out a brochure explaining why information security is important and how employees take part in maintaining a high security level would not work in fast message speed societies. In fact, a mixture of both is probably the best approach. The awareness of employees in slow message speed cultures should be raised by fast message speed messages but important background information should be provided at the same time. The same is true for information security policies. They should be presented together with the big picture, especially in slow message speed and high-context societies. In fast message speed and low-context cultures, they can also be set and published as rules that the employees need to stick to. Since many countries, especially in Europe, have a rather slow message speed but are low-context at the same time, it is difficult for security managers to find the right balance.

A common mistake is that security awareness material is just copied from the headquarter in the United States or Europe. This material often shows Caucasians actors in a Western setting. Sometimes even the content is only understandable by people from the culture in which it was produced. Companies should try to adapt such material to the target culture by choosing actors that represent a typical mix in the company or even in the target country. Local specifics, like laws, stereotypes, software, references to local celebrities, etc. should either be eliminated or adapted to the target country. I once saw a security video that built its entire message around the German concept of privacy, starring only Caucasian actors in a private office space and which referred to the German minister of the interior by his name and not even by his position. It was shown to Chinese employees in an open-plan office who, of course, did not understand the reference to the German politician and were confused by the entire video. Adaption is crucial for the success of security awareness campaigns.

6.9.3 Concluding Remarks

The direct impact of the preferred message speed on information security seems rather limited. There is an influence based on the way relationships are built and the way information (for example in security awareness campaigns and trainings) is transferred. Security managers need to adapt their material but also their way of transporting the message (for example by regular repetition or by continuously providing further information) to the local culture.

6.10 Rating: The Impact of Individual Dimensions

After analyzing Hofstede's and Hall's cultural dimensions and their influence on information security and after supporting those insights by triangulating them with findings from research in aviation safety and a profound literature review, a researcher's story has been told and an exciting field for future

research has been opened. However, this thesis not only addresses the international research community but should also serve as a source of inspiration and even a guideline for practitioners. I would like to partly fulfill this obligation by rating the cultural dimensions according to their influence on information security. This enables me to derive an information security country rating purely based on cultural characteristics. I decided to only use Hofstede's dimensions for this rating in order to assure consistent results. Hofstede focused on cultural values, which describe the cultural characteristics of groups and change only slowly. To make full use of Hall's dimensions, one needs to analyze two parties because his dimensions are focused on the interaction between two individuals or groups. This thesis focuses on China and therefore only offers one perspective. Furthermore, Hofstede assigned country scores for various countries to his dimensions. These scores can be used for comparing countries. Hall describes his dimensions on an abstract level and provides examples for individual countries but does not derive quantifiable scores. He neither assigns country scores nor clusters a large number of countries. I will therefore use Hall's dimensions afterwards to provide some additional insights but do not use them for the rating itself.

6.10.1 The Scale and the Influence of Hofstede's Dimensions

I use a scale to rate the impact of Hofstede's characteristics. The scale ranges from -5 to $+5$ and has the following meaning:

-5 This cultural characteristic has a very negative influence on information security.
0 No direct relation between this cultural characteristic and information security could be identified or positive and negative influences on information security seem to level out.
$+5$ This cultural characteristic has a very positive influence on information security.

As mentioned above, Geert Hofstede's cultural characteristics are rated on this scale. Assigning a *+5* to a particular characteristic means that this characteristic has a very strong positive influence on information security. A *+2* means that this characteristic also positively influences information security but the impact is smaller than for the former one. This categorization is based on the findings I described throughout this chapter. It can be seen as a summary of the sections above. The rating is a first approximation that should be scrutinized and adjusted in the future. In section 7.3.9, *Improved Country Risk Model*, I present possible paths for further research. One important improvement would be to base the rating on quantitative research. For now, we will work with this first hypothesis. Out of the nature of the research that was conducted for this thesis (qualitative exploratory research), the scores cannot be proven right or wrong. All I can offer is a variety of evidence that supports

my arguments. This evidence has been presented throughout this chapter. As we will see later, my results are greatly aligned with the findings of researchers in the field of aviation safety.

Power Distance $= -4$

> Power Distance has an influence of -4 on information security. This means that it has a strong negative influence on information security. If the power distance is high, this is likely to lead to severe information security risks. Low power distance has a positive effect.

Individualism $= +4$

> Individualism has an equally strong influence on information security. However, it positively correlates with a high level of information security. Individualist societies provide a more secure environment than collectivist societies.

Masculinity $= -1$

> Masculinity has a slightly negative effect on information security. The influence of this dimensions is significantly lower than for power distance and individualism.

Uncertainty Avoidance $= 0$

> Uncertainty avoidance seems to have an influence on information security. However, as we could see in section 6.4, there are situations in which strong uncertainty avoidance has a positive effect on information security but there are also examples of the opposite effect. Therefore, this dimension is rated as neutral.

Long-term Orientation $= /$

> Long-term orientation is excluded from this rating. It only has an indirect influence on information security which overlaps with the other dimensions. Furthermore, Hofstede's country ratings conflict with the behavior I observed in the outsourcing industry in China. People in rural areas and on China's economic center along the East coast show very different behavior. A country comparison using Hofstede's country score for this dimension therefore seems too simplified.

In the following, the results are compared to findings in the field of air traffic safety.

6.10.2 Comparison with Air Traffic Safety

Joseph L. Soeters and Peter C. Boer, both from the Department of Social and Behavioral Sciences at the Royal Netherlands Military Academy, empirically analyzed the correlation between cultural characteristics and accident ratios in military aviation. They based their insights on Hofstede's cultural dimensions. In their paper *Culture and Flight Safety in Military Aviation*,[158]

---

[158] See Soeters and Boer (2000)

they state the following partial correlations between accident ratios (1991-1995) and Hofstede's cultural characteristics, controlled for the contribution of technical failures as a cause of accident:[159],[160]

Power Distance .63
Individualism −.89
Masculinity −.06[161]
Uncertainty Avoidance .75

Their results greatly overlap with my findings. They also found that a large power distance increases the likelihood of incidents and that a strong tendency towards individualism reduces it. When they conducted their research, Soeters and Boer did not expect a relation between masculinity and air traffic accidents. Their data also does not show any correlation between masculinity and accident ratios. The slight difference to my results can be explained by differences in the working environment. Since flight crews change regularly, roles are rather clear and competition might be less fierce. Also changing airlines is not as easy as changing employers in the outsourcing industry so that the effect of turnover is smaller. When pilots change airlines, they find a similar environment because security procedures are supervised in this industry. The only dimension that is significantly different to my findings is uncertainty avoidance. Soeters and Boer see a strong correlation between uncertainty avoidance and air traffic accidents. They argue that personnel with a low uncertainty avoidance have less trouble reacting to unknown situations. In the field of air traffic, that is highly important if one has to handle unanticipated threats. The disrespect for formal rules, high turnover and strong patriotism, all related to low uncertainty avoidance, have a negative influence on information security. The creativity and flexibility normally related to low uncertainty avoiding societies is suppressed in China by its education system and the high power distance. Since I primarily focused on China, a country with an extremely low score for uncertainty avoidance, the correlation between uncertainty avoidance and information security is not clear. It should be scrutinized in further research. For now, it seems to have a neutral effect.

Due to the similarities between the fields of aviation safety and information security, Soeters and Boer's results underline my findings. Three out of four dimensions, power distance, individualism and masculinity, have a similar influence on information security as on air traffic safety.

---

[159] Those results therefore focus on human error as the cause of accident.

[160] For their research approach and the validity of their results, see Soeters and Boer (2000).

[161] They state that his correlation is the only one that is not significant, based on their data.

6.10.3 Edward T. Hall's Dimensions and their Influence on Information Security

Not only Hofstede's but also Edward T. Hall's dimensions have an impact on information security. However, while Hofstede's dimensions can describe an individual culture based on values, Hall's dimensions are important when people from two different cultures interact. Communication is the main focus of Hall's dimensions.

Context orientation is the dimension that is most closely related to information security. A list of cultural characteristics linked to this dimension has been described in section 6.6. It is directly linked to the perception of privacy, the meaning of contracts, the way negotiations are conducted, etc. Also the way outsourcing partnerships are managed is highly dependent on the country in which the services are outsourced. Those examples show that the dimension itself does not have a strong direct impact on information security – neither negative nor positive. However, it plays a pivotal role for establishing and managing outsourcing deals. Based on the distance in context orientation, one can predict difficulties in communication and take countermeasures (adapts one's behavior) even before running into those problems. Outsourcing from extreme low-context cultures like Germany to high-context cultures like China and Japan is difficult. Companies from the United States, outsourcing to India, should have less communication problems because the gap in context orientation is smaller.

On the other hand, examining India from a *time orientation* perspective (*monochronic versus polychronic time*), it is a rather difficult country to outsource to. Its time perception lies between multi-active and cyclic. For linear-active cultures, like the United States and Germany, it is therefore more difficult to communicate and cooperate with Indian than with Chinese or Japanese. Of course, time orientation is only one dimension and many other characteristics like a language barrier also play an important role in communication. However, for negotiations, schedules, deadline, etc. the impact of this dimension should not be neglected. If a German company would outsource to South America – from a linear-active culture to a multi-active one – the problems are likely to be severe. Those differences in time orientation should be considered before deciding where to outsource.

Out of Hall's dimensions, the perception of *space* is the dimension that seems to have the most direct impact on information security. It influences the usage of office space but also the perception of privacy in cultures and thereby in companies. Open-plan offices and a low sense of privacy can lead to a multitude of security problems if they are not properly taken care of. Especially in open-plan offices, a set of physical but also organizational countermeasures should be established and strictly enforced. Without those measures, confidentiality of sensitive data is at risk.

Hall's last dimension, *preferred message speed*, only has a limited influence on information security. It only leads to minor communication problems

in negotiations and influences the way of establishing partnerships. However, security managers should be aware that successful communication of security awareness campaigns and security trainings is related to the way messages are decoded. If employees have a cultural background that prefers slow decoding of messages, this message format should be chosen and vice versa. But as I mentioned, the impact of this dimension is limited and should only play a minor role for selecting the outsourcing location and adapting to its culture.

Since Hall's dimensions are primarily focused on the interaction between two cultures, they are not integrated into my model that rates the security level of countries based on its cultural characteristics. However, they can be used as a second step. After calculating the security level of a country and going through the list of potential security threats based on Hofstede's characteristics, one can look at one's own communication patterns and compare it to the target country. If there are large gaps concerning Hall's dimension, they should be taken into consideration and one should anticipate potential communication problems. By being aware of those challenges, one can develop a strategy of how to react to them.

6.10.4 Concluding Remarks

Practitioners, but also researchers, can use the rating of Hofstede's cultural dimensions to cluster countries and rate them according to their level of information security purely based on cultural characteristics. Furthermore, it can be used for screening potential outsourcing providers. By analyzing the cultural characteristics of a provider's employees, potential problems can be predicted and risks managed. When a certain characteristic is identified, one can refer to the section above that is dedicated to this characteristic. This helps researchers and practitioners to understand its influence. Thereby, potential problems can be addressed and countermeasures introduced.

In the following section, I rate the countries that we focused on in this thesis based on the scale above and thereby evaluate their level of informations security. Of course, culture is not the only factor determining a high or low level of information security in a country but can provide a first glance at potential risks. It also allows the analysis from a perspective that has largely been neglected up to now.

6.11 Country Comparison: Culture-based Information Security Evaluation

Since I rated the impact of each of Hofstede's dimensions on a scale from -5 to $+5$[162] and because Hofstede derived country scores for each of these

---

[162] PDI = -4, IDV = 4, MAS = -1, UAI = 0, LTO was excluded

dimensions, calculating a rating of our focus countries is fairly easy. Information security scores for all other countries that Hofstede evaluated can be calculated without any adaptation of the model.

For calculating the country score of a country X, one only needs to put Hofstede's values into the following formula:

$$-4(\text{PDI}(X)-50)+4(\text{IDV}(X)-50)-1(\text{MAS}(X)-50)+0(\text{UAI}(X)-50)^{163}$$

Please note that Hofstede's scores are normalized so that they are always between 0 and 100.[164] A negative multiplier like -4 for PDI means that a high power distance has a negative effect. A power distance of 50, which is neither high nor low, should not have any effect on our country score. Thus I subtract 50 from each of Hofstede's country scores. If a country scores low on a dimension (for example Germany on PDI = 35), the country score adjusted by 50 is negative. This negative score (low power distance) multiplied with a negative multiplier results in a positive effect of this dimension (Germany: $-4\cdot(35-50)=-4\cdot-15=60$). Therefore, Germany receives points for its low power distance because low power distance has a positive effect on information security. An information security country score of 0 means that its culture does not have any influence on information security (compared to the world average).[165] The higher the score, the stronger is the positive influence of a country's culture on information security. A negative score means that the culture implies information security risks.

According to Hofstede, China shows the following cultural characteristics: PDI = 80, IDV = 20, MAS = 66, UAI = 30. By putting these scores into the formula, we derive an information security country score of -256 for China.

$$-4(\text{PDI}(X)-50)+4(\text{IDV}(X)-50)-1(\text{MAS}(X)-50)+0(\text{UAI}(X)-50)$$
$$-4(80-50)+4(20-50)-1(66-50)+0(30-50)$$
$$-4(30)+4(-30)-1(16)+0(-20)$$
$$-120-120-16$$
$$-256$$

By putting in Hofstede's country scores for all countries, we derive the following information security ratings: China $= -256$, India $= -122$, Japan $= -77$, Germany $= 112$, USA $= 192$. The scores for these countries are visualized in figure 6.8.

---

[163] I did not exclude uncertainty avoidance here because it seems to have an impact on information security. Further research can reveal if its impact is really neutral (0) or if another value is more appropriate.

[164] Country scores that were derived after his main study, might be above 100. However, this is not the case for any of the scores used here because I excluded long-term orientation on which China scores 118. Amongst the countries we focus on, it is the only score above 100.

[165] Of course, it does have an influence. However, this is how I adjusted the scale. Negative and positive influences level out.
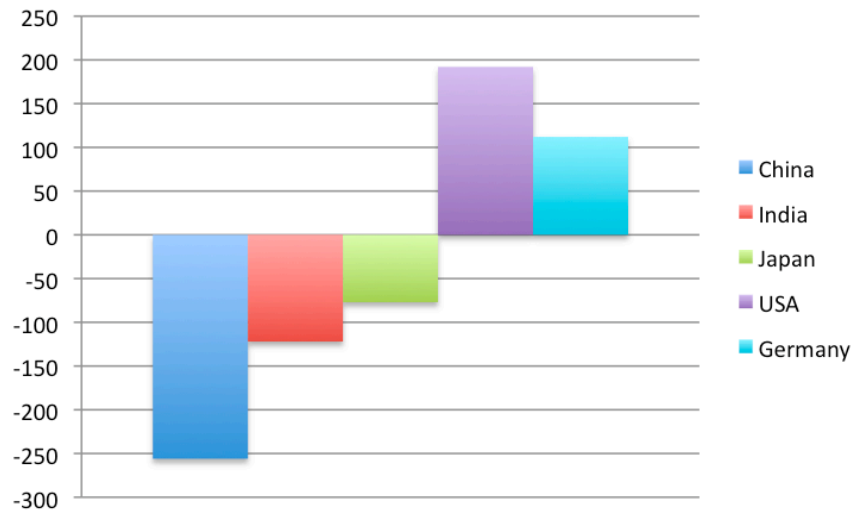
Fig. 6.8. Country Comparison: Culture-based Information Security Evaluation

Purely based on cultural characteristics, China seems to provide the most insecure environment. In India and Japan, one can expect significantly less culture-based security problems than in China but still a lot more than in Germany and the United States. By focusing on Hofstede's dimensions and excluding Hall's cultural characteristics, the United States provide the best cultural conditions for a high level of information security.

As mentioned earlier, one could use Hall's dimensions for adjusting this information security rating. The perception and usage of space suggests that the value for the United States should be lowered and the German value increased. Since open-plan offices are very common in the United States, doors are normally open and the importance of privacy is lower than in Germany. This might change the ratings. However, because Hall did not provide any country scores and because mixing scores from two different researchers can lead to consistency problems, Hall's dimensions should rather be used in a qualitative manner. One should be aware that they are not taken into account in this model and should review what kinds of problems they might cause.

6.12 Tools for Culture-sensitive Outsourcing

After introducing a large number of concepts and after evaluating culture-related security threats, I would like to give a brief overview of how executives, risk managers and security managers can combine these insights in order to outsource in a culture-sensitive manner. Figure 6.9 outlines how the insights of this work can be incorporated into established outsourcing practices. It

shows a possible combination of the methods and insights that I presented in this chapter. However, it is only one way of using the different methods. It does not cover all tools that I introduced and the displayed tools can also be combined in a different order or with different information flows.

Furthermore, please note that the outlined process only covers a very small part of the entire outsourcing process. Due diligence has to cover many other aspects besides cultural risks and there are many outsourcing-related security risks that are culture-independent.[166] The figure only shows how the various culture-related tools I introduced can be combined. By following this process, outsourcing clients will be able to better manage culture-related security risks.

Let me go through the process step by step: At the beginning of the outsourcing process, after a company has decided to outsource a set of services, it needs to find a suitable outsourcing location.[167] As the first step, one could use the culture-based security rating I just introduced. Hofstede's dimensions are available for a large number of countries and his scores can directly be put into the formula above.[168] Afterwards, one could calculate the culture distance between the own and potential target countries.[169] Thereby, one knows the security risk of the target countries (based on their cultural characteristics) and can directly see how different the cultures of those countries are (compared to the own culture). The larger the culture distance, the more likely one will encounter intercultural clashes. The culture distance can be calculated as an aggregate or for each of Hofstede's dimensions. Since all these results are purely based on Hofstede's cultural dimensions, they can be adjusted by means of Hall's cultural characteristics. If one lives in a low-context country, outsourcing to a high-context country could lead to security problems. The same is true if there are large differences in the perception of time (linear-active, multi-active and cyclic; monochronic versus polychronic).[170]

For understanding the cultural differences and resulting security threats, one can always refer to the respective section of this thesis. This would be the second step of the country selection. One could review Hofstede's and Hall's cultural characteristics for each target country. If the countries exhibit extreme scores on one or more dimensions, one can plunge into the respective section and see what kinds of security problems might arise out of these cultural characteristics. With this background knowledge, and after completing the other parts of the due diligence process that should be carried out at the same time, one has a sound fundament for choosing an outsourcing location.

---

[166] In section 3.2.1, I presented a large number of indicators that can be used to evaluate and compare different countries. Chapter 4 lists many outsourcing risks that are rooted in China's social, political and business environment. Similar problems exist in many other countries as well.

[167] As I said before, the country selection demands an analysis of many different factors. This process only addresses those that are culture-related.

[168] See section 6.11

[169] See section 6.1.6
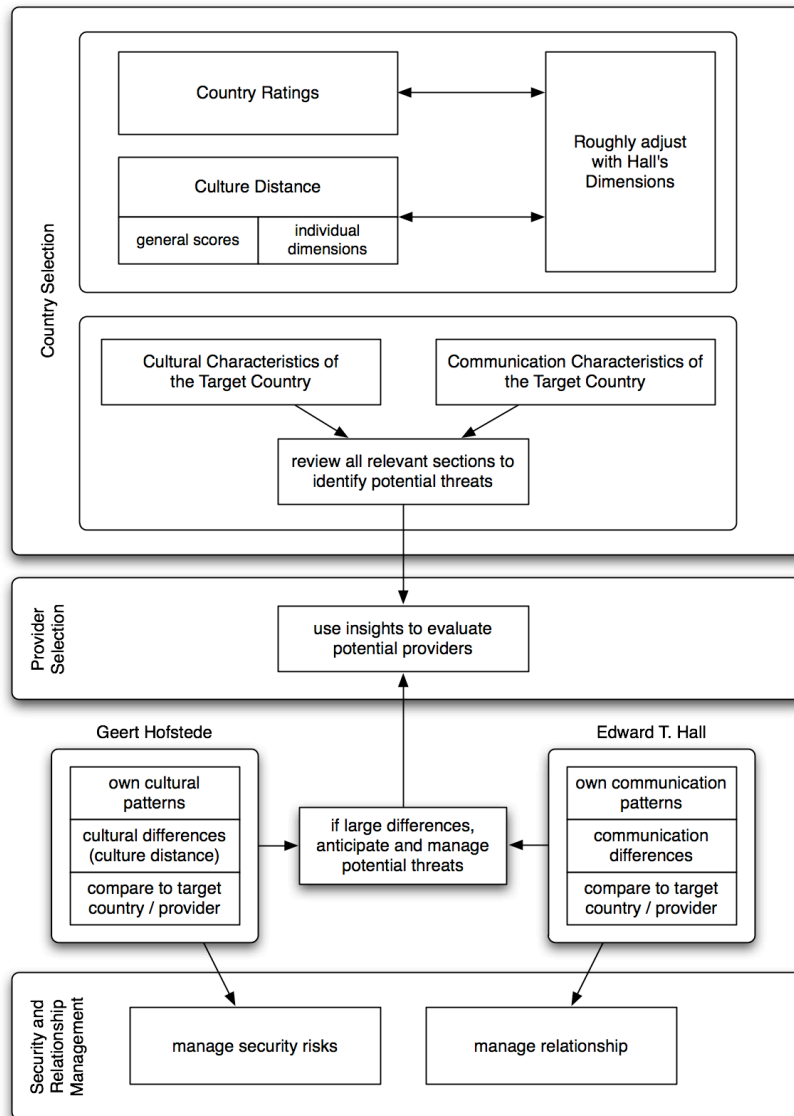
[170] See section 6.7

Fig. 6.9. Culture-sensitive Outsourcing – Using the Toolbox

The second phase of the outsourcing process, the provider selection, builds on many of the insights one has gained during the country selection. Up to now, a large problem has been that security manager did not know what kinds of culture-based security threats they should look for when scrutinizing potential providers. By looking at the cultural characteristics of the providers' countries and after reviewing the respective sections, security managers get a feeling for the security problems they might encounter. With this knowledge, they can directly assess the outsourcing providers. They can check if they find some of the security issues, evaluate how the providers handle them and can judge if these risks can be managed properly in the future. A second, more time-consuming method could be applied as well. If the potential providers seem to be multicultural companies, one could cooperate with them and jointly assess their employees. By deriving cultural scores specific to the providers' employees (based on Hofstede's and Hall's dimensions), one could get a detailed picture of all outsourcing providers, culturally independent from the countries they operate in.

As the last step of the provider selection, one should analyze the cultural characteristics of the own company (according to Hofstede and Hall). This assessment will show cultural differences and communication differences between the own company and potential providers (or the outsourcing locations). If large differences become apparent, one knows that problems are likely to arise and can come up with strategies of how to mitigate these problems. The results can directly be used for the provider selection.

As I mentioned at the beginning of this thesis, outsourcing as well as security management are continuous processes. The last phase of the outlined process, managing security risks and the the relationship with the outsourcing provider, is a never-ending effort. Of course, all the insights that were gained during the two previous phases (country and provider selection) can and have to be used in this last phase as well. The findings should be reviewed regularly because assumptions as well as the personnel of both companies are likely to change. As a general tendency, the findings based on Hofstede are likely to support the security management efforts, results based on Hall's dimensions will improve the outsourcing relationship.[171]

Using these tools will help to anticipate and manage culture-related security threats. For this reason, they will also improve the due diligence process – the country and the provider selection in particular. However, the other parts of the due diligence remain highly important. A culture-based assessment can only enhance the process and cannot replace other evaluations.

In this chapter I offered a toolbox. Each manager can select the tools he finds most appropriate. When one or a few of them are used in the presented or in a similar manner, security risks can be lowered. Moreover, the entire

---

[171] Please note that Hofstede's dimensions also shine light on the relationship and Hall's dimensions on potential security problems. However, generally, they will rather help to mitigate the problems as shown in figure 6.9.

outsourcing relationship is likely to be more successful because the responsible managers will become more aware of cultural differences.
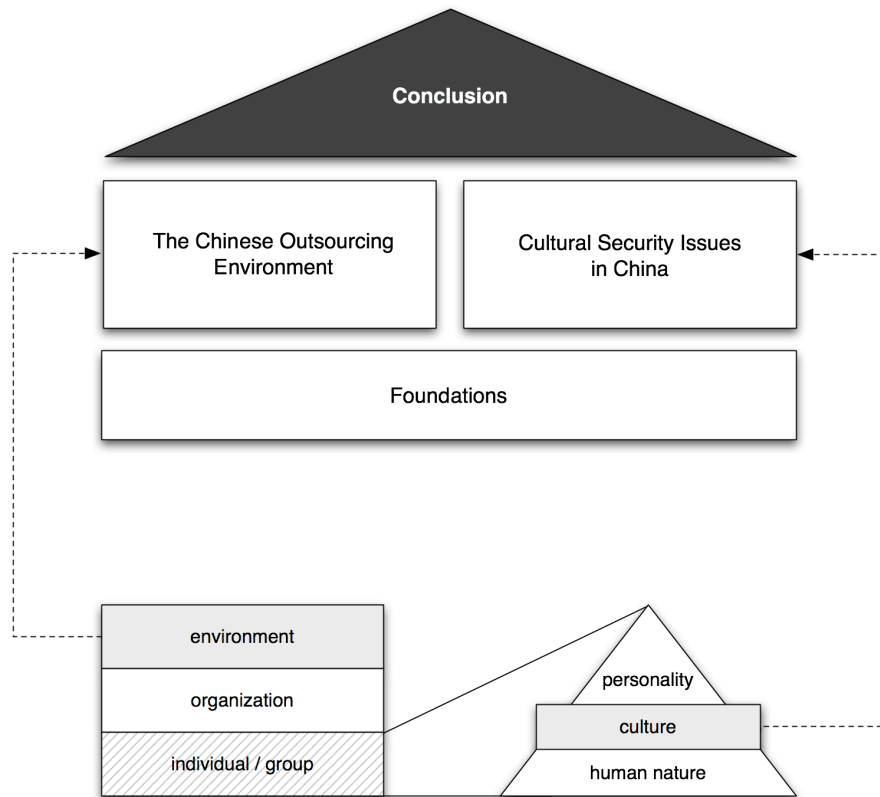
6.13 Concluding Remarks

This chapter was devoted to the presentation of my findings on culture-based security threats. As we saw earlier already, the human factor plays a crucial role in information security. With the necessary background in cultural studies, we had a framework for analyzing the impact of national cultures on information security. Three of Hofstede's cultural dimensions (PDI, IDV and MAS) seem to correlate with information security threats. One dimension needs to be scrutinized further (UAI) and one should be adjusted and new data should be collected to examine if there is a correlation with information security (LTO). Based on these dimensions, I have built a model that can be seen as a first step towards ranking countries on their cultural preconditions for information security. China seems to provide a more insecure environment than India and Japan. The United States and Germany provide positive cultural characteristics supporting information security. But the model is not limited to these countries. It can be applied to any country that was analyzed by Hofstede or that is scrutinized using Hofstede's dimensions. This provides a new perspective for risk managers who analyze potential security threats endangering their outsourcing ambitions. Even without using the country model, by identifying the cultural characteristics of a country, potential security threats can be predicted. This chapter provides insights for each dimension. The model is not even necessarily limited to countries. Scrutinizing the cultural characteristics of a region or even a company's employees can provide insights into their behavior which might help to discover potential security threats. In outsourcing deals, two different cultures interact with each other. Even two Chinese companies have different corporate cultures which might result in miscommunication. For analyzing those communication problems, I introduced Edward T. Hall's cultural dimensions. By filling each dimension with empirical insights that I discovered during my problem-centered interviews in China, I tried to raise the understanding of security threats that result out of problems in the interaction of two different cultures. Especially an analysis of context orientation but also time orientation, and to a lesser extent the other two dimensions,[172] can provide insights into security risks that can be expected when dealing with cultures that show a large difference to the own. The entire model, the country risk model but also the information regarding culture-based security threats, is far from being

---

[172] Like Hofstede's dimensions, space and preferred message speed can better be used for understanding security threats within a culture than explaining the interaction between cultures. However, they also show how security practices might differ between cultures and that they need to be adapted.

perfect or exhaustive. It is a first step towards recognizing culture as an important factor in information security. Further research needs to be conducted in other countries to view this topic from other perspectives, without the bias of China's cultural characteristics. I would like to initiate a rethinking of information security, integrating researchers from other disciplines, especially from human sciences, to participate in the discussion. This leads me to the broader implication of my work.

Part IV

Conclusion

Conclusion

The Chinese Outsourcing Environment

Cultural Security Issues in China

Foundations

environment

organization

individual / group

personality

culture

human nature

7

Conclusion

After a thorough analysis of the Chinese outsourcing environment and the impact of culture on information security, I would like to round up my work by presenting its broader implications. Afterwards, I summarize the research process and the major findings of this thesis. I draw out its limitations and highlight starting points for further research. In the end, I recapitulate on the significance of this thesis for the future of China's outsourcing market. I explain how the results can be used for circumventing sour surprises.

7.1 Broader Implications

I started this thesis because I wanted to understand why the Chinese outsourcing market feels like a market for lemons. The quality of outsourcing providers is perceived as low and that feeling adds to the decline in quality of the market players. However, by trying to understand why managers are afraid of outsourcing their IT services in and to China and why they give poor ratings to outsourcing providers in China, I discovered an entire new field of research. This thesis has implications way beyond the outsourcing industry. This section is devoted to a brief description of the implications of this thesis.

7.1.1 Reducing the Information Asymmetry

I was striving to understand the fear of managers to outsource in and to China and I found various reasons for them to be afraid. The understanding of China, Chinese culture and how to conduct business in China, is fairly poor – even among expatriates who live in the People's Republic. Chinese culture is seldom embraced but rather feared. By examining the outsourcing sector in more detail, it becomes obvious that many outsourcing problems are not unique in China but are faced by companies all over the world. There is an information asymmetry between outsourcing providers and their (potential) clients. This situation is worse in China because of the lack of knowledge

about Chinese business practices. There are many bad stories about conducting business in China and a lot of managers base their judgement on hearsay. The information asymmetry is extremely hard to reduce, especially if the outsourcing provider does not favor reducing it. Foreign managers often do not trust Chinese certificates. A serious screening procedure demands many resources. Analyzing the behavior of an outsourcing provider's employees is almost impossible. By linking cultural characteristics to security threats, I offer a framework that can be used for gaining a broad overview of the security level of different outsourcing destinations. Furthermore, it provides security managers with a list of potential security threats that they should look for when selecting an outsourcing provider. Thereby, they can predict problems that are likely to occur when choosing particular providers. This can either influence their outsourcing decision or tell them what kinds of countermeasures they should employ for solving those problems. By offering researchers and practitioners a culture-based model for analyzing security risks, I reduce the information asymmetry between providers and their clients. Moreover, my methods can be employed even within a firm. Hofstede's dimensions are developed for analyzing national cultures. However, they can be applied to any other kind of culture (regional cultures, corporate cultures, etc.) in the same way. If security managers and risk managers collect data about their own or their outsourcing provider's employees, they can better understand them and their behavior.

7.1.2 Doing Business in China – The Environment

In the course of gaining insights about culture and information security, I became aware of many conditions in the business environment in China. I found reasons, other than the information asymmetry and cultural distance, that account for the fear of managers. I presented country risks like the economic, social and political instability that China faces. I wrote about China's legal system and the infrastructure that China deployed over the past couple of decades. I also presented the role that the media plays in China. All those insights form an overview of China's business environment. Even though they are focused on the outsourcing market, they are still general enough to be highly interesting for almost anybody doing research or business in China. The information is not only applicable to the outsourcing market but caters all kinds of business professionals.

7.1.3 Outsourcing Practices

I hope and believe that some companies that outsource their IT services will listen to my advice. If they do, they will adjust every single phase of their outsourcing process. They will include cultural aspects into the considerations of how and what to outsource, the evaluation of potential outsourcing providers, the management of the outsourcing partnership and also the evaluation of the

outsourcing deal and eventually its termination. Managers will use my country risk rating for comparing different outsourcing destinations. They will look at links between cultural dimensions and information security to predict and to react to potential security threats. Highly important, but often forgotten, they will look at Hall's cultural characteristics and change the way they approach and afterwards interact with their providers. Culture plays a central role in outsourcing, not only (but of course very strongly) for offshoring deals. Even when nearshoring or inshoring, there are cultural differences that need to be addressed throughout the entire outsourcing life cycle.

7.1.4 Broadening the Understanding of Information Security

Besides outsourcing, I hope that I achieved a very ambitious but in my opinion crucial goal. I wanted to broaden the understanding of information security. Information security cannot be assured by purely technical or organizational measures anymore. With continuing decentralization, the human factor plays an increasingly important role. More research needs to be conducted on the edge between information security and social sciences. A small group within the international research community is starting to embrace this view. Research on the economics of information security and on psychology and information security is starting off. Those activities should be strongly supported. I would like to add another path to this trend. A new perspective that I believe will become more and more important in a global business world. Sociology and cultural studies can provide an understanding of human behavior that is necessary to implement efficient and effective security measures. Furthermore, they are necessary components for building a new security paradigm. Ideally, information security should be self-regulated, without a central force. The invisible hand can become the future of information security. If that is the case, we need to have a deep understanding of human behavior to learn how this market might function.

7.1.5 Changing Security Practices in General

By highlighting the importance of culture in information security, I believe that not only security practices related to outsourcing but information security practices in general will be adjusted. Standards in the field of information security (e.g. ISO/IEC 27001, ISO/IEC 27002, BSI IT Baseline Protection Manual) largely neglect the impact of culture on information security. Culture is hardly mentioned as a direct or indirect factor. The same is true for practices in the field of information security. During the past years, I have seen the security concepts of many small and large corporations. Almost none of them acknowledged that culture plays a role. Even the importance of the human factor in general is still largely ignored up to now. Security training and awareness campaigns are only found in large organizations. Even there,

they are not tailored to the target culture but developed in the headquarter and thereafter shared with subsidiaries in other countries. Today, cultural diversity within organizations is extremely common. Global partnerships all over the world (and omnipresent information exchange with partners) demand not only an understanding of the other country's legal environment but also of its culture. Risk and security managers are seldom aware or even trained in intercultural issues. Culture should be an integral part of their training so that they can include cultural specifics into their risk evaluations and security concepts. National and international security standards should raise the awareness of cultural issues in information security by addressing them directly. Exchange of best practices between companies, also focusing on cultural aspects in information security, should be supported by the management. Information security professionals need to understand human behavior and should therefore understand basic principles of economics, psychology, sociology, cultural studies, etc.

7.1.6 Concluding Remarks

The implications of this thesis go way beyond the scope of outsourcing. They are also not limited to China. Those two limitations were just the scope chosen for the empirical analysis. Human behavior does play a major role in information security. Security managers had to have technical expertise in the past. Today, management skills are seen as more important.[1] In the future, we will see more and more security managers with a background, or at least sound knowledge, in social sciences. Understanding human behavior is key to effective security concepts. Social sciences provide us with a solid method set for gaining this knowledge. By making use of these methods, we can gain insights that are necessary to assure information security in the future.

7.2 Summary

The goal of this thesis was to explore the impact of (national) culture on information security. I wanted to examine the relations between the disciplines of cultural studies and information security. This topic came up during the time when I lived and studied in Shanghai. I realized that managers have an enormous fear to outsource in or even to China. Due to this fear, the quality of outsourcing providers seemed to deteriorate or at least not develop – outsourcing in China could be seen as a market for lemons. I wanted to understand this fear and examine if it is justified. Therefore, I decided to analyze outsourcing relationships in China. Besides the motivation to understand the

---

[1] Of course, a profound understanding of technical issues is still necessary. However, technical knowledge is not sufficient for implementing a sound security concept anymore.

outsourcing market and its security problems, there were three other reasons for me to embark on this journey and to analyze the Chinese outsourcing market. The first reason was rooted in business, the other two research-focused. Even though China is still seen as the world's factory, it is stepping up the value chain. China is increasing its market share in the outsourcing sector. Outsourcing IT services in and to China is therefore becoming increasingly important. From a business point of view, the outsourcing sector is gaining importance and needs to be understood properly. The second reason for choosing this scope is based on the research conditions and opportunities that the outsourcing sector exhibits. By analyzing the relationship between outsourcing providers and their clients, I could clearly observe the information asymmetry between those two parties. Sometimes, the provider is interested in keeping this asymmetry as large as possible. However, even if it wants to reduce it, this is extremely difficult. *Signaling* does not work if certificates are not trustworthy. *Screening* is extremely time-consuming, and thereby expensive. The information asymmetry also exists within companies. Managers do not understand the intention and the behavior of their employees. Therefore, any approach that helps reducing this information asymmetry is highly valuable – for outsourcing deals but also within companies. For observing the information asymmetry and how relationships should be managed, examining outsourcing relationships seems like an excellent choice. Roles and responsibilities are defined more elaborately than within firms. The third reason for selecting this scope was also research-motivated. By analyzing outsourcing relationships I could even observe the interaction between different cultures and problems that arise out of those cultural differences.

In order to understand the relations between cultural studies and information security, I needed a research scope that allowed me to examine differences in culture. In outsourcing deals, it is common that people and companies from various countries interact. By choosing the outsourcing scope, I could gain insights into how cultural differences influence relationships and how they create security problems. By plunging into the Chinese outsourcing sector, I could reveal the real situation that outsourcing clients face and generate first insights into the impact of culture on information security.

7.2.1 Conditions and their Indicators

Before analyzing security threats, I reviewed the conditions for outsourcing in China and India. For comparing these two countries, I chose four fields: *General Human Development*, *Education*, *Use of Communication Technology* and *Governance*. On the *Human Development Index*, China ranks 82nd compared to India ranking 128th. This means that the Chinese society is generally 'more advanced' than the Indian. Concerning education, the illiteracy rate of Chinese aged 15 years or older was only 9.1 percent in 2007 (compared to 39 percent in India). The percentage of Chinese enrolling and graduating in secondary and tertiary education is significantly higher than amongst Indians.

Regarding the availability and use of communication technology, India also trails China. As a percentage of the population, there are less people in India than in China who have access to telephones (landlines and mobile) and the Internet. Data from the Worldwide Governance Indicator project reveals that both, China and India, still have a long way to go towards an environment of good governance. Both countries rank significantly lower than the United States, Germany and Japan on all major indicators. India ranks slightly higher on some dimensions but overall, India and China are almost on the same level. Since the environment plays a significant role for outsourcing decisions and many security risks are related to environmental factors, I described it in an own chapter.[2] Reviewing the conditions for outsourcing in both countries, the clear preference of many managers towards India is surprising. The lower language barrier is likely to play a role. However, concerning environmental indicators, China and India seem to provide a similar environment. In many fields, China even offers better conditions than India. After a systematical analysis of security risks, we can judge if the managers' fear is reasonable.

7.2.2 Potential Security Threats of Outsourcing Deals

The outsourcing risks companies face can be clustered into three layers: *Environmental forces*, *Organizational forces* and *Individual and Group forces.*[3] The first layer (environmental forces) describes the political situation, legal regulations, etc. that companies should take into account when choosing an outsourcing destination. The second one (organizational forces) is focused on particular outsourcing providers. It consists of risks due to their financial (in)stability, (in)experience, etc. The third level describes problems that occur on the human level. Those security threats can be based on the behavior of individuals or on team dynamics. This third level can be subdivided again into three layers: *human nature*, *culture* and *personality*. During due diligence, most companies focus on scrutinizing the environment (environmental risks) and potential outsourcing providers (organizational risks). The third level (individual and group) is rarely analyzed. One of the reasons is that the behavior of an outsourcing provider's employees is almost impossible to observe. However, there are theories in other disciplines that can help to gain an understanding of potential security threats based on human behavior. Those disciplines are, amongst others, economics, psychology, sociology and cultural studies. For solving the problems I saw in China, I decided to gain a deeper understanding of the cultural level. The entire organizational level was less promising because the insights vary from provider to provider. Models for analyzing outsourcing providers on this level already exist but can only provide an understanding of individual firms. To generate insights that are useful to a large audience, I decided to describe my findings on two levels: the environmental and the cultural level (as part of the individual/group

---

[2] See chapter 4
[3] See section 2.4.3

layer). I described the environment that China creates for outsourcing and how this environment supports certain security threats. However, the fear of outsourcing in and to China is not only related to the environment. The fear of Western companies to outsource their IT services is also largely based on unknown cultural characteristics. Therefore, culture, as a part of the third layer of potential security risks (individual and group forces), is the second and main level I focused on in this thesis.

7.2.3 The Chinese Outsourcing Environment

On the environmental level, there are various deficiencies in China that can be seen as potential security threats. One is the lack of stability that China shows on three different but highly interlinked fields. It lacks economic, social and political stability. China's financial system is overstrained by bad loans and its currency needs to be revalued. The transition from state-owned to privately-owned enterprises is in progress and leads to social problems (major layoffs, cost cutting, ownership disputes, etc.). These social conflicts are also problematic if China does not maintain its current growth. As long as every member of society sees its income grow each year, social stability can be maintained. Income disparities, which are growing, can become serious sources of social unrest if a growth of the own wealth is not evident anymore. However, high growth rates also lead to an increase in demand and rising prices – inflation is the result. Inflation and a revaluation of the Chinese currency would deteriorate China's position as an export and outsourcing location. A last field that shows how interlinked economic and social stability are is the growing pressure on China to take care of the environment. The Three Gorges Dam forces many Chinese to relocate and China's industry pollutes the environment in ways that make large areas uninhabitable. Naturally, this leads to social unrest. Many Chinese have to leave their families and work as migrant workers in coastal areas. This creates a social disruption that is seething underneath the surface. A still high level of corruption makes matters worse. Many ordinary citizens are not properly compensated for burdens posed onto them by the government or the industry. Corruption and local dictatorship also lead to political instability if people feel mistreated. Regions like Xinjiang, Tibet or even Taiwan are in ongoing conflicts with the administration in Beijing. The border between economic, social and political risks is blurry and problems in one area lead to problems in the others.

Many stability issues are further linked with China's immature legal system. China is on the path towards the rule of law. The Chinese administration has initiated some major improvements in this field after China's accession to the WTO. However, China has still a long way to go. Relationships play a major role in Chinese culture and often overrule formal agreements. Corruption is therefore hard to come by. A lack of basic conditions makes matters worse. In many cases, companies and researchers report conflicting legislation, poorly trained judges and lawyers, lack of transparency, etc. With a largely corrupt

legal system and strict regulations on private and commercial investigation, legal agreements with own employees and outsourcing providers are hard to enforce (e.g. non-disclosure agreements and Service Level Agreements).

Poor infrastructure and restrictions in the telecommunication and security industry are other environmental risks. Officially, the use of cryptography is tightly controlled. China has repeatedly tried to force own standards (for example WAPI). Those standards might support wiretapping by the Chinese administration. If the Chinese administration could decrypt traffic even on the fly, filtering encrypted traffic would become possible and thereby this traffic could also be examined by the Great Firewall (China's large perimeter content filter). Even unintentional misconfiguration of this filter can render services unavailable. But the risks of unavailability of services does not only lie in China's security mechanisms but also in its Internet infrastructure itself. With only three major choke points for traffic leaving the country, the infrastructure cannot cope with failure of one of the links. This became a serious problem in December 2006, when an earthquake in front of the Taiwanese border disrupted international links to China. Restrictions in the telecommunication industry create similar problems on the domestic scale. Few telecommunication firms are allowed to offer services in China and they have regionally clustered the market even today. Between the networks of these providers are choke points, similar to the ones at China's borders. The lack of highly educated technicians leads to unavailability of services. This can hardly be circumvented by changing providers because of the strict market regulation.

The media, which should reveal many of these problems, also cannot unfold its full potential because of strict regulations in the media industry. Since all mass media is censored, media can hardly influence legislation and cannot reveal problems within firms. Security issues are rarely covered so that the general public is not sensitized for security risks.

The environmental forces just described can all be seen as security risks. They can threaten the confidentiality, integrity and availability of information within companies and therefore within outsourcing relationships as well. My interviewees were worried about those risks but their largest fear arose out of their lack of understanding of the Chinese culture.[4]

7.2.4 The Impact of Culture on Information Security

For understanding the impact of culture on information security, we first had to take a look at previous research conducted in this field. By doing so, I could show that the impact of culture on information security has hardly been discussed up to now. If researchers found any relation to cultural studies at all, their focus was on information security culture. However, information

---

[4] Even the Chinese interviewees, who were mostly educated abroad or worked for Western companies, were worried about how Chinese culture creates security threats.

security culture is about creating an environment in which secure behavior is demanded by values and norms. An information security culture is an organizational culture that is established as a security measure by continually educating the employees in the field of information security. It therefore greatly differs from the impact of culture on information security, which is about analyzing national, regional, but also organizational cultural characteristics and scrutinizing how these support or undermine secure behavior. For properly analyzing those issues, based on a sound foundation, I had to review research in the field of cultural studies. I needed a framework that enabled me to study the topic in a structured manner with a profound understanding of the field of cultural studies.After reviewing the work of many cultural researchers, I decided to focus on the work of Geert Hofstede and Edward T. Hall. Geert Hofstede is probably the most renowned researcher in the intercultural domain. Almost all major cultural researchers build upon or at least acknowledge his work. He developed five cultural characteristics that can be used for describing (national) cultures – *power distance*, *individualism*, *masculinity*, *uncertainty avoidance* and *long-term orientation*. Edward T. Hall has a different focus. He mainly worked in the field of intercultural communication. The cultural characteristics he analyzed are *context orientation*, *monochronic versus polychronic time*, *space* and *preferred message speed*. Like Hofstede, he is a highly renowned researcher with many followers building upon his work. I chose the work of these two researchers as my framework mainly for two reasons. My interviews showed that security threats are based on two different cultural conditions. They can be attributed to the behavior of a single individual or can arise in the interaction of two parties with different cultural backgrounds. The first setting is covered by Hofstede, the second one by Hall. Moreover, Hofstede's as well as Hall's characteristics have been reviewed thoroughly by the international community. Deficiencies of their studies are known and can be reacted upon.

My results show that a high power distance in a society can lead to security threats. In high power distance societies, employees do not disagree or criticize their superiors. It is against their cultural characteristic to scrutinize the intentions or the behavior of others with a higher social status. Furthermore, corruption and bribery are more common in high power distance societies. Rules are less important than relationships. This directly leads us to the second characteristic, which is highly interlinked with power distance – individualism. China is an extremely collectivist society (low individualism). Concepts like face, harmony and strong patriotism play an important role. Collectivist culture are mostly shame cultures, as compared to individualist guilt cultures. People in guilt cultures tend to stick to rules because they would otherwise feel guilty. In shame cultures, the social punishment that is executed on wrong-doers is the stronger social regulator. Collectivist cultures therefore demand a different security approach and more oversight. Like a high degree of power distance, collectivism has a negative impact on information security. In masculine societies, there is an immense pressure on young men to strive

and become successful in their jobs. This leads to internal conflicts and high turnover, especially in knowledge-intense fields like the IT outsourcing sector. The impact of masculinity on information security is less direct and weaker than for the first two dimensions. However, strong masculinity can be regarded as a security risk. During my interviews in China, I found many security incidents that seem to be related to Hofstede's uncertainty avoidance dimension. However, some are related to a high degree of uncertainty avoidance, others happen in low uncertainty avoiding environments. Therefore, this dimension was rated as neutral. Its impact on information security should be scrutinized further in form of a quantitative study. Long-term orientation only seems to have an indirect influence on information security. If people are long-term oriented in business environments, it can have a positive influence. However, if their long-term orientation is more directed at their social network or the nation as a whole, it can lead to security threats because bribery and nationalistic behavior are more likely. Hofstede did not split this dimension into these two aspects and no data is available for these more specific applications. Long-term orientation was therefore excluded from further analysis.

Hall's dimensions also have an influence on information security. However, their impact is more indirect. They play a highly important role in the interaction between two parties. These parties can be a manager and his or her subordinate, two colleagues, but also an outsourcing provider and one of its clients. In high-context cultures, communication is process-oriented. Relationships are deep and play a highly important role. They are established over a long period of time. Sensible topics are not addressed directly but communication slowly leads to the core of a request or a debate. In low-context cultures, communication is rather goal-oriented. Therefore talk is straight-forward and problems are addressed directly. Relationships are less important than in high-context cultures. This can lead to difficulties in communication and misunderstandings. The role of contracts is largely different in high-context compared to low-context cultures. The entire outsourcing relationship is seen from two divergent perspectives. These diverging assumptions lead to problems in the relationship and in communication. The result can be security incidents. The perception and usage of time can be categorized as monochronic or polychronic (or linear, multi-active and cyclic). It does not seem to have a strong influence on information security. However, it does play a role in the way negotiations are handled and relationships are seen. A stronger influence on information security has the conception of space. It is largely differs from culture to culture and determines the office layout but also the perception of privacy. Especially if the conception of space leads to a usage of office space that is counterproductive to information security or if it weakens the importance of privacy, additional security measures need to be deployed. The preferred speed at which we send and receive messages plays an important role in communication. Especially security awareness campaigns but also other security-related communication needs to be adjusted to the target environment. When interacting with people from another cultural environment, one should be aware

of cultural differences and adapt to the communication scheme of the other party. The larger the cultural differences are, the more difficult can be the communication with an outsourcing provider. In order to circumvent security threats resulting from miscommunication and different views on relationships (and how they should be handled), outsourcing clients need to take these differences into account when analyzing potential outsourcing destinations. During the provider selection process and the entire outsourcing relationship, these differences need to be kept in mind and addressed.

To provide researchers and practitioners with a model that is easy to use for analyzing different cultural environments and judging their information security level, I assigned security-impact scores to each of Hofstede's dimension. The findings are not final and should be seen as a first step towards a culture-based security rating. The results can be applied to national cultures but also any other form of culture. Based on my findings, I derived a score of -4 for power distance, 4 for individualism, -1 for masculinity and 0 for uncertainty avoidance. Multiplied with Hofstede's country scores and adjusted as described in section 6.11, I derived ratings for five countries: China $= -256$, India $= -122$, Japan $= -77$, Germany $= 112$, USA $= 192$. This means that purely based on cultural characteristics, China shows most security risks, the United States provide the most secure environment.

I excluded Hall's dimensions from this rating. However, a comparison of the own culture with the target culture based on Hall's characteristics should be done after reviewing the country rating. The results of the rating can be adjusted based on these differences in communication. Even though China is rated worst amongst the countries I compared, it might be the most suitable outsourcing destination for many Asian countries because of similarities in communication and other cultural characteristics.

It is most important to be always aware of cultural differences. Thereby, one can predict security threats and implement countermeasures. Furthermore, by adapting to the other party's cultural characteristics, one can build up a successful and long-lasting outsourcing partnership.

7.2.5 Triangulation with Air Traffic Safety

The results I derived in the field of information security were compared to the field of air traffic safety. The impact of culture on air traffic safety shows strong analogies to its impact on information security. Since the outcome of air traffic incidents can be lethal and because the field of air traffic is inherently international (and therefore intercultural), many researchers have analyzed the correlation between cultural characteristics and air traffic accidents. Research in this field is also mostly based on Hofstede's cultural characteristics. Various researchers managed to replicate his results in the air traffic industry. Furthermore, they found that some characteristics rise and others lower the risks of air traffic accidents. High power distance and a low degree of individualism (collectivism) can lead to safety threats, for example. Those results

match with my information security findings in the outsourcing industry and therefore support my results. As it was done in air traffic studies, a quantitative research approach could be applied in future research and provide further insights on the impact of culture on information security.

7.2.6 Concluding Remarks

The impact of culture on information security has hardly been analyzed up to now. This thesis shows that culture plays a highly important role in information security and that this role is becoming increasingly important as businesses take more and more advantage of globalization. The results of my research show how culture and information security are interlinked and which characteristics are likely to lead to security risks. This work was meant to start a discussion about the role of culture in information security research and should provide first insights. Furthermore, the results of this thesis should also help managers to understand China as an outsourcing destination. There is a strong fear of outsourcing in and to China. This fear is rarely based on facts but is rather a feeling. I therefore analyzed outsourcing risks in China in a structured manner. Outsourcing can incur security risks on three different levels. There can be environmental risks, organizational risks and individual/group risks. This thesis describes risks on the environmental level and further analyzes security risks on the individual/group level with a focus on culture. I hope that I added a valuable path to the future development of information security research and substantiated the outsourcing discussion by providing managers with information about China as an outsourcing location.

7.3 Limitations and Further Research

As with any other form of research, this thesis cannot cover all aspects of the topic in the largest possible depth. I cannot possibly look at the problems I raised from all potential perspectives. I believe that my research approach enabled me to incorporate ideas, concepts and perspectives from an unusually large number of disciplines. However, it was necessary to find a scope that made it possible to analyze the problems and to present the results in a holistic manner within a limited time frame. While conducting primary and secondary research, many new ideas and perspectives came up that I mostly tried to incorporate. Nevertheless, as the hermeneutic approach teaches us, there is always room for improvement. It is always possible to gain a broader or deeper understanding of particular aspects of a problem. Whenever I saw limitations during this thesis, I pointed them out. In this section, I would like to summarize these limitations and propose new starting points for future research.

7.3.1 My Cultural and Personal Bias

Every form of research is biased. I grew up in Berlin, Germany, and lived there for a large part of my life. Afterwards, I broadened my horizon by living in various other countries and experiencing various new cultures. Since I lived in China for many years, this country made the most profound impression on me. Spending time in Great Britain, Switzerland and Ghana, as well as many other countries I visited, was also very important for my personal development and my understanding of cultural differences. I feel like a European and this is probably how my cultural bias can be described. Even though I believe that I learned a lot about Chinese culture, I will never understand it as Chinese do. I cannot thoroughly understand certain concepts because I did not experience them from my early childhood on. Besides my German (or European) cultural background, I got my own personal bias. It is formed based on the experiences of my life. This view of the world is different from the view of anybody else. My cultural and my very personal bias, both often indistinguishable from one another, are also incorporated in my work. They are impossible to remove. The personal bias of a researcher is always present in his research. Even though I was as objective as possible in my judgements by thoroughly reviewing other researchers' work and basing many claims on reproducible indicators, this bias does affect my research. Not only do the data collection method and my way of analyzing data from primary and secondary sources reflect my personal bias, even the fact that I discovered and chose the research questions of this thesis are due to my personal preference. This bias cannot be removed and does not make this work less valid. It is just a bias that readers need to be aware of and that they should reflect while and after reading.

7.3.2 The Research Approach

During the last couple of years, I spent a lot of time reading about and experimenting with different research approaches. After long consideration, I formed my research framework out of various different pieces. This framework is thoroughly described in appendix A and I spare you from describing it once again. I was looking for a research approach that allowed to broaden the field of information security research without focusing on particular problems in too much detail. The approach had to generate results that are trustworthy on one hand but also non-final. It was clear that further research would adjust my findings and generate a more holistic picture and a deeper understanding of my research questions. Therefore, I decided to follow an approach that can be described as qualitative exploratory research. This approach was ideal for its purpose. I believe that I received holistic and sound results. However, together with the research approach, I also inherited some limitations. Many of the limitations that are sketched out during the rest of this section are based on my research approach. However, for reaching my research goals and answering my research questions, the approach was most appropriate.

7.3.3 Country Bias – Looking through Chinese Glasses

Some of the limitations of my work emerged out of the scope that I chose. I decided to focus on outsourcing of IT services in and to China. This enabled me to provide specific examples instead of opening a purely theoretical discussion. Furthermore, it generated practical insights for researchers and practitioners alike. However, it also limited my view and accounts for a bias that my research exhibits.

Based on a profound literature review in the field of cultural studies and personal experiences in other countries, I generalized some of my findings. However, one needs to be aware that the expert interviews were solely conducted in China and that the entire research process is focused on understanding culture-based security threats in the People's Republic. Since I linked particular security incidents present in China with the underlying cultural characteristics and because Hofstede and Hall provide us with data on other countries, the findings can be transferred. If a security threat seems to exist due to China's high power distance, we can expect the same threat (maybe with minor variations) to be present in other high power distance cultures as well. However, because I did not conduct any primary research in other countries, the validity of this generalization cannot be proven. Furthermore, I was only able to find those security threats that persist in China. Due to China's specific combination of characteristics, some threats might be suppressed there. Other threats might not exist in other countries even though the primary characteristics that they were attributed to show similarities to China.

The same is true for the assignment of values to Hofstede's dimensions. Since data was mainly collected in China, some security threats that I found might also be based on other factors than purely Hofstede's characteristics. If that is the case, the actual impact of individual characteristics might not be judged correctly. Whereas I am confident that the general judgement is correct (e.g. high power distance = negative, high individualism = positive),[5] the actual degree (value from −5 to +5) might be over- or underrated.

All those potential inaccuracies can be reduced by analyzing a larger set of countries. By doing so, more information becomes available. This information will reveal whether my results can be generalized or if they are specific to China.

7.3.4 Limited Number of Threats

Also due to the research methodology and the country focus, the list of culture-based security threats is limited. In order to derive a larger set, researchers should follow two complementary paths. First, the number of interviews can be increased and the interviews can be solely focused on culture-based security

---

[5] The triangulation with air traffic safety provides supporting evidence.

threats. Now that we know what kind of risks to look for, the interviews can be conducted more focused, narrowing the scope and thereby reducing the efforts needed for each interview. By increasing the number of interviews, the number of identified security threats is likely to increase as well. However, since many of the threats that my interviewees revealed were stated repeatedly towards the end of my data collection phase, I am confident that I identified the major security threats that are related to cultural characteristics in China. Nevertheless, there could be many more and different threats in other regions and countries. Conducting interviews in Hong Kong, Macau and Taiwan, or even in other countries all over the world, is likely to reveal new threats. Conducting interviews in other regions and countries is the second path that can be followed by future research. Both approaches will lead to a longer list of security threats. Even today, practitioners can look at the section of this thesis that covers a characteristic that they are interested in. Thereby, they will find a list of culture-based security threats that they are likely to face. Further research, adding more security threats to these lists, will add value because more threats can be anticipated and reacted upon.

7.3.5 Replicating Hofstede

My country ratings, but also the rest of the analysis, is based on Hofstede's country scores to a large extent. In the past, Hofstede's scores have been criticized for being mostly derived from respondents within one company, IBM. Furthermore, Hofstede's surveys took place many years ago.[6] Therefore, replication studies using Hofstede's framework, deriving new country scores, would be useful for strengthening the fundament of this thesis. New scores might lead to minor adjustments of my findings. However, since Hofstede's work is based on values instead of practices, and values change only very slowly (over a long period of time), we can assume that his country scores are still valid today and accurate enough for our purpose. This argument is supported by the fact that recent replication studies in specific industries have derived results very similar to Hofstede's.

7.3.6 Individual Dimensions

Individual dimensions that I presented in the course of this thesis need to be scrutinized further. Uncertainty avoidance, for example, needs further research. I found a positive but also a negative impact of uncertainty avoidance on information security. Therefore, I rated the dimension neutral for now. However, research in the field of air traffic safety suggests that a high degree of uncertainty avoidance makes people less flexible – unable to react to unknown situations. Researchers in this field therefore suggest a correlation between uncertainty avoidance and air traffic accidents. A similarly strong

---

[6] For a discussion of Hofstede's research approach and his results, see section 6.1.5

impact as in air traffic safety could not be observed in the field of information security. It is unclear if this is due to differences between air traffic safety and information security or due to my research focus on China. China scores extremely low on uncertainty avoidance. This might be a reason for only finding very few security threats linked to high uncertainty avoidance. Only further research (more interviews and research in other countries) can clarify the role of uncertainty avoidance. Also Hofstede's long-term orientation dimension needs to be analyzed further. It would be interesting to split this dimensions into long-term orientation towards business (employer) and private life (society). After this split, those two dimensions might lead to diametrical results. Since there is no reliable research on the impact of long-term orientation on air traffic safety, also changing the perspective to air traffic safety does not provide us with further insights. For masculinity, it would be interesting to analyze countries that score extreme on this dimension. Most countries we looked at have a rather moderate country score on masculinity. Therefore, the impact of masculinity on information security cannot be observed as easily as on dimensions with high or low scores. Primary research is needed to understand the influence of uncertainty avoidance and long-term orientation (and also partly masculinity). It can also provide a stronger fundament for all other dimensions.

7.3.7 Integrating other Dimensions

In this thesis, I focused on Hofstede's and Hall's cultural characteristics. This decision is thoroughly explained in section 6.1.4. However, this does not mean that the usage of other researchers' dimensions is not appropriate. On the contrary, I am certain that the analysis of culture-based security threats based on the frameworks of other cultural researchers can generate extremely insightful results. Other dimensions can provide new perspectives. Different cultural researchers have different focuses and clustering security threats based on other dimensions can shine light on further links between culture and information security that are hidden up to now. I therefore encourage further research based on Hofstede's and Hall's cultural characteristics but also strongly support the application of frameworks of other cultural researchers.

7.3.8 Analyzing the Interaction of Countries

As proposed above, future research should analyze cultural characteristics and their impact on information security in other countries. Furthermore, the interaction between different cultures and the impact of cultural differences on information security should be analyzed more closely. This was started in this thesis but was mainly done as a theoretical discussion. When going through Hall's cultural characteristics, I highlighted how the interaction of different cultures can influence information security. Those insights could be supported by additional empirical evidence. More insights can be gained by

observing the interaction of individuals and groups, from different regions and countries. It would be interesting, for example, to observe problems when outsourcing from linear to multi-active environments.[7] Therefore, the focus of future research should not only lie on traditional outsourcing destinations (and their clients' countries) but also include Mediterranean, South American and Arabic countries. Those exhibit strong multi-active behavior, which has not been analyzed up to now. The same can be done with Hall's other dimensions respectively. My discussion of Edward T. Hall's dimensions provides a starting point for further research in this field.

7.3.9 Improved Country Risk Model

As I said before, my country risk model, which describes the security level of a country purely based on cultural characteristics, is only a first step into this direction. There are three major improvements that I suggest for future research to enhance my model and its results. First, new dimensions can be integrated into the model. These new dimensions can cover cultural aspects that Hofstede's dimensions cannot grasp. Thereby, the model could become more holistic. Second, the assignment of security risk values to cultural characteristics should be based on quantitative research.[8] Thereby, the Chinese bias of my model could be eliminated and more exact scores could be derived. The third path does not only correct deficiencies and make the model more precise but generates a new model. By quantifying and integrating intercultural dimensions like Hall's into the rating, a model could be built that not only describes security risks within one country but quantifies risks that occur in the interaction of two countries. This model could take two countries as an input and calculate a score that describes the likelihood of security incidents when organizations from these two countries interact. This last step could also be done without building a new model. As in this thesis, dimensions that describe problems in intercultural communication can be examined after security scores for a set of countries have been calculated. Managers (and researchers) can use these insights to adjust the results in a quantifiable manner or just mentally. However, I believe that the most important step is the second one. Quantitative research should be conducted in various countries. Empirical data can be used for validating and adjusting my first insights on the impact of particular cultural characteristics on information security. With a broad qualitative view and focused quantitative data, a sound model can be built that can be used for comparing information security all over the world.[9]

---

[7] The interaction does not necessarily need to be limited to outsourcing. The observation of any other form of interaction can be very insightful as well.

[8] Please look at respective work in the field of air traffic safety.

[9] One could also build a model integrating many more characteristics than purely cultural ones. One could for example combine indicators from all three levels (environment, organization, individual/group) and build an even more holistic model

7.3.10 Concluding Remarks

This thesis offers broad insights on outsourcing in China and on the impact of culture on information security. However, there are also many limitations that are based on the research approach or the fact that I mainly focused on one country, China. Please note that this thesis is only a first iteration on the hermeneutic spiral. It is not meant to provide final results. On the contrary, I would like to initiate a rethinking of information security by adding insights from the field of cultural studies into the equation. Information security researchers and practitioners should review concepts and findings from cultural studies, but also sociology, psychology, etc. Thereby, they can broaden their understanding of their own field. My goals are not diminished by the limitations just presented. Those limitation rather provide interesting starting points for further research.

7.4 More Than Lemons

Many managers are afraid of outsourcing their IT services within or even to the People's Republic of China. The outsourcing market in general is a market for lemons. It is extremely difficult for companies to assess the quality of service providers in advance. They are trapped in the principal-agent problem. Outsourcing providers are often not interested in revealing their actual level of information security. Even if they believe that they provide high-quality services, it is hard for them to convince potential clients. This situation is even worse in China because the trust in institutions is lower than in many other countries. The environment, which is unknown to many foreigners, is judged badly based on hearsay. Therefore, signaling and guarantees – certificates and Service Level Agreements – do not work. Managers are afraid of faked certificates and an immature legal system that makes it impossible to enforce contractual agreements. Screening is extremely difficult because of language differences and cultural barriers. The human factor is gaining importance in the field of information security. Unfortunately, it is even harder to analyze than organizational aspects. Without a proper understanding of the environment and without a way of assessing the quality of an outsourcing providers' staff, companies can only resort to one criterion. Their decision is mostly based on trust.

---

describing information security in various countries. However, by integrating these factors (as it is already sometimes done today), new data must be collected continuously. Since values change only very slowly, a security rating based on cultural characteristics can be built once and is valid for many years. Since Hofstede calculated scores for many countries worldwide, scores for all these countries can be derived without collecting any new data. Since culture does influence all other levels, it can be assumed that a culture-based rating already exhibits aspects that are normally clustered as environmental or organizational.

By analyzing outsourcing relationships in China, I could shine some light on the actual outsourcing environment that China provides and the role that the human factor plays in information security. By reviewing the conditions that China offers (its education system, the dissemination of communication technology, etc.), it becomes obvious that it can certainly compete with countries like India. However, the current environment still has to improve. China has to gain stability, the legal system needs to mature and Chinese protectionism, especially in the telecommunication sector, has to be dismissed. Despite those problems, China seems to be on the right track. Its accession to the WTO has initiated and stimulated improvements in many of those sectors. If known, companies can react to many of these problems. Some can be circumvented, others need to be accepted. But if anticipated, the related risks can be assessed and managed. By understanding the environment, we start to understand the rules of the market – rules that seemed very foreign at the beginning. By understanding the rules, we sense how to deal with them. Eventually, we might even be able to trust this market.

More difficult than understanding the market is the assessment of the human factor and its role in the security of outsourcing deals. If it could be judged properly and companies would include this assessment in their due diligence process, the information asymmetry could be reduced. Deep within the large heap of lemons there are some delicious cherries hidden. Those cherries need to be found and picked for the Chinese outsourcing market to cultivate. Until we find a way to steer information security by means of the invisible hand, or until the invisible hand sorts out the cherries from the lemons, we need to find method for finding out what is happening within those fruits. We need to understand how employees behave and why they behave in a certain way. There are promising approaches in economics and psychology to understand human behavior and its impact on information security. This thesis adds a new piece to this puzzle. A new path, that needs to be walked in order to deepen our understanding of human behavior. Sociology and cultural studies are disciplines that offer an enormous method set and an ocean of knowledge that we only need to tap into. By following this new path, we can gain knowledge about our own organization and potential providers. By adding this piece to the puzzle, we get a more holistic picture and start seeing the differences between lemons and cherries. If we continue our journey, we will see that the Chinese outsourcing market offers more than lemons. We will find the cherries we are looking for.

Appendix

A

Methodology – An Empirical Study of Security Risks

This thesis opens a new field of research combining methods and insights from cultural studies with the field of information security research. Such an interdisciplinary work raises the question how insights are acquired and validated. This part of the appendix is meant to explain my research methodology and my reasoning. It provides background information that has not been presented in the course of the thesis.[1] In the following I will answer four core questions:

1. What are the main research paradigms that are followed?
2. Which methods are chosen to gain insights and to base research claims upon?
3. Why are the the results trustworthy?
4. How are the methods applied specifically during the research?

A.1 Methodology

The term *methodology* can be interpreted as *"body of practices, procedures, and rules used by those who work in a discipline or engage in an inquiry"*.[2] I do engage in an inquiry. My goal is to understand and to describe how national and regional cultures influence information security. I analyze how security issues can be mapped to and explained by looking at cultural characteristics and I scrutinize whether certain security issues can be predicted by analyzing cultural characteristics of employees. In order to reach my goal, I employ a set of methods and follow a certain scheme that is described in this section. I further not only describe the methods I chose but also explain my decisions. Where appropriate, I compare different research practices and

---

[1] This part can be referred to at any stage of the reading process. I suggest skimming through it after the introduction and a thorough read before starting chapter 4.

[2] See Pickett et al. (2000)

outline the scope of my research. I structured the description of my research setting according to the following scheme (figure A.1).
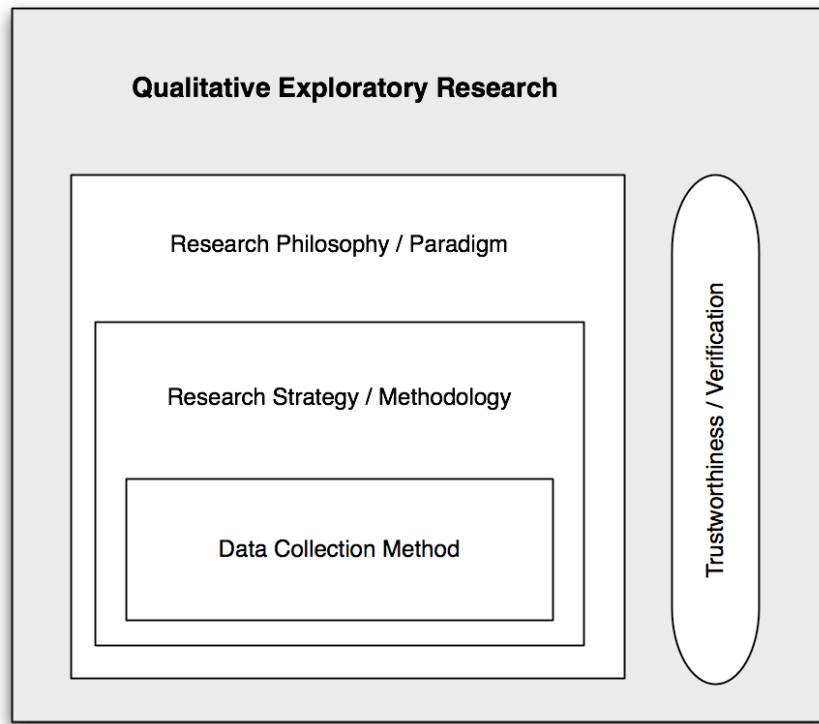

Fig. A.1. Structure of my Research Approach

I will first talk about the general research idea and afterwards about its underlying research philosophy.[3] How this philosophy is implemented is described as the research strategy[4] which itself makes use of a particular data collection method.[5] Since I work empirically, trustworthiness of my research design is a highly important issue. I will address it in a specific section[6] and along the presentation of my results.

---

[3] See section A.1.2
[4] See section A.1.3
[5] See section A.2
[6] See section A.1.1

A.1.1 Qualitative Exploratory Research

The research that underlies my thesis can be described as *qualitative exploratory research.*

"*Historically, there has been a heavy emphasis on quantification of science. Mathematics is often termed the 'queen of sciences', and those sciences, such as physics and chemistry, that lend themselves especially well to quantification are generally known as 'hard'.*"[7] On the other hand, there are 'soft sciences', social sciences in particular. Quantification of science in research field was often said to go along with scientific maturity.[8] When more and more researchers enter a particular field and when economic decisions are made based on their research, decision makers demand quantitative data.[9] This is because numbers have power to persuade readers of their credibility.

British philosopher, economist and politician John Stuart Mill "*is said to have been the first to urge social scientists to emulate their older, 'harder' cousins, promising that if his advice were followed, rapid maturation of these fields [...] would follow.*"[10] Across all fields of science, it became more and more common to start with a hypothesis and to either verify (positivism) or falsify (critical rationalism) it. The second approach, falsifying a given hypothesis, has been advanced by Austrian philosopher Karl Popper.[11] His thoughts are best summarized in a quote by Stephen W. Hawking:

> No matter how many times the results of experiments agree with some theory, you can never be sure that the next time the result will not contradict the theory.[12]

Whichever approach is being followed, either verifying or falsifying a predefined hypothesis, both are deductive and normally quantitative in nature. To work deductively, it is necessary to have a broad and deep knowledge of the field in question. Therefore, quantitative research is often criticized for not generating new knowledge but rather verifying existing theories. Quantitative insights strip the context and might only be applicable in certain situations, under assumptions (or certain values of variables) that might not be stated in the research design because they were forgotten or disregarded by the researchers themselves. Hence, quantitative research might lack generalizability.[13] Furthermore, it does not seem to be appropriate for understanding human behavior. Quantitative data can describe the 'behavior' of physical objects and might lead to insights but can hardly explain "*the meanings and*

---

[7] See Guba and Lincoln (1994, p. 105)
[8] See Guba and Lincoln (1994, p. 106)
[9] See, for example, Sechrest (1992, p. 3)
[10] See Guba and Lincoln (1994, p. 106)
[11] See, for example, Popper (2002, p. 46 ff.)
[12] See Hawking (1998, p. 10)
[13] See Guba and Lincoln (1994, p. 106)

purposes attached by human actors to their activities".[14] It is normally collected in a predefined environment in order to validate a certain hypothesis but not for discovering new knowledge. When looking for insights into new fields, qualitative research has gained prominence again and reverted the progression of social sciences, and even so called 'hard' sciences, back from quantitative to qualitative methods.

This entire thesis is *descriptive* and *explorative* for the very reason that it opens up a new field of research, combining social sciences with computer science, in order to explain information security issues. It therefore needs to follow a qualitative paradigm. Its purpose is to convince the reader that classical thinking in information security is not adequate, considering upcoming challenges like a growing cooperation with partners and outsourcing of production and services. Information security researchers and practitioners need to look into other disciplines to explain and tackle information security issues that were not present a few years ago. Economics can be seen as one of those disciplines that offer interesting insights into information security issues. A couple of years ago, most researchers disregarded economics because they believed it could not offer anything valuable for the field of information security. It was not until highly renowned researchers and practitioners like Hal Varian, Ross Anderson, Bruce Schneier etc. came together and started a small conference on the links between information security and economics, the *Workshop on Economics and Information Security* also known as *WEIS*. The same is true for other disciplines in social sciences today. They have not been linked with information security issues up to now. Security researches have not entered those disciplines yet. However, there is a whole new field to explore, with valuable insights for research and practice.[15]

When researchers discover new research problems, entering entirely new areas of research, they have to decide whether they would like to analyze one particular aspect in depth or rather open up the new field for other researchers to build upon their work. I do explore a new field of research, opening the discipline of cultural studies to information security research. I decided to focus on analyzing characteristics of national cultures, as a field of cultural studies, and to open this field as broad as I can. Of course, my research builds on various sources in the field of information security research and cultural studies. However, there has not been any serious preliminary work linking those two fields that I can base my research on. Therefore, I can only describe what I observed and explore this new field as I experienced it. Nevertheless, I do follow a research strategy that focuses on assuring the trustworthiness of my research so that other researchers can safely build upon my work.

Whenever I make a claim, it is based on a reasoning that I will reveal simultaneously. This reasoning might already convince most readers. However, to also convince the skeptical or rather highly critical reader, I will further

---

[14] See Guba and Lincoln (1994, p. 106)
[15] For further insights, see section 5.1 and section 5.2

support my arguments by basing them on hard evidence. I collected evidence that strongly supports my case. If I came across evidence that was in conflict or even contradictory with my claims and reasons, I either explained those conflicts and resolved them or I scrutinized my claims and dropped them.[16]

It is highly important to accept the fact that whatever methodology one builds his arguments on, whether the applied methods are quantitative or qualitative, the claims one makes, the hypothesis promulgated can seldom be *proved* valid. However, I will explain in detail how I would like to assure that my readers will understand and accept my reasoning – not only persuading them by founding my claims on reasons and evidence but also revealing my entire research strategy and the reasons behind my selection of particular research methods.

Trustworthiness of Qualitative Research

Researchers following a qualitative approach often need to defend themselves, especially regarding the *trustworthiness* of their research.

Egon G. Guba and Yvonna S. Lincoln, both highly renowned researchers in the field of qualitative research, have identified and suggested four aspects that 'prove' the soundness or trustworthiness of qualitative research.[17] Qualitative research should be measured against each of those concepts. If all four criteria are fulfilled, the examined research can be regarded as trustworthy. Those four criteria are:

Credibility Do the findings presented in this thesis accurately reflect the reality studied?
Transferability Are these findings useful for to others in similar situations?
Dependability Would the results be repeated if the study was replicated?
Confirmability Do the data help confirm the findings?[18]

Guba and Lincoln derived those concepts from four major concerns relating to trustworthiness:[19] *truth value*, *applicability*, *consistency* and *neutrality*.

Computer science is still often considered to be a 'hard science'.[20] Therefore, many researchers still follow a quantitative approach. If one wants to address people, one needs to be able to speak their language, not only concerning national languages but also professional expressions and jargon. In order to open up my thesis to a broader audience, including researchers with

---

[16] See Booth, Colomb, and Williams (2003, p. 115 ff. and p. 138 ff.)

[17] See Guba (1981); Lincoln and Guba (1985); Guba and Lincoln (1994, 2005)

[18] The specific, very concise descriptions of the concepts are adopted from Björck (2001, p. 7 f).

[19] See Guba (1981, p. 79 ff.)

[20] This categorization might be due to its relations to mathematics.

a background in hard sciences, I added table A.1 which translates those terms I just introduced to the terms that quantitative researchers are familiar with.[21]

Credibility stands for *internal validity*, the qualitative term *transferability* can be regarded as *external validity* or *generalizability*, *dependability* is the more appropriate term than *reliability* and *confirmability* represents *objectivity*.[22]

Aspect	Scientific Term	Naturalistic Term
Truth Value	Internal Validity	Credibility
Applicability	External Validity Generalizability	Transferability
Consistency	Reliability	Dependability
Neutrality	Objectivity	Confirmability

Table A.1. Scientific and Naturalistic Terms Appropriate to the Four Aspects of Trustworthiness, as in Guba (1981, p. 80)

In order to achieve trustworthiness (credibility, transferability, dependability and confirmability), Guba, and later Guba and Lincoln, came up with a strategy. They defined a set of methods that support the trustworthiness according to each criteria. A summary of their approach is shown in table A.2.

In the following, I will go through each criterion and the related methods in order to explain how I achieved trustworthiness of my results.

Credibility

There are five main methods for establishing credibility of research results: *Triangulation*, *Member Checks*, *Persistent Observation*, *Peer Debriefing* and *Establishing Referential Adequacy.*

Sandra Mathison, Professor of Education at the University of British Columbia Vancouver,[23] said in 1988 that *"good research practice obligates*

---

[21] This table is copied from Egon G. Guba, who also tried to close the gap between qualitative and quantitative research in his 1981 paper *Criteria for Assessing the Trustworthiness of Naturalistic Inquiries.* See Guba (1981)

[22] Lincoln and Guba write about the naturalistic paradigm and about qualitative methods that are applied for making naturalistic inquiries. It is important to note that naturalistic and qualitative are not synonyms as well as rationalistic research does not need to be quantitative. Naturalistic inquiries can be made in a qualitative manner as well. However, in practice, research following the naturalistic paradigm is so often conducted qualitatively and rationalistic research using quantitative methods that we do not need to make that distinction here. See Lincoln and Guba (1985) and Guba and Lincoln (2005, p. 200 f)

[23] Her research focus lies on *Evaluation Theory* and Qualitative Research.

Criterion	Methods	Findings are
Credibility	Triangulation	Plausible
	Member Checks	
	Persistent Observation	
	Peer Debriefing	
	Establishing Referential Adequacy	
Transferability	Theoretical/Purposive Sampling	Context-relevant
	Collect a lot of Data	
Dependability	Overlap Methods	Stable
	Stepwise Replication	
	Audit Trails	
Confirmability	Triangulation	Investigator-free
	Practicing Reflexivity/Audits	

Table A.2. Achieving Trustworthiness of Naturalistic Inquiries, based on Guba (1981, p. 83)

the researcher to triangulate, [...] regardless of which philosophical, epistemological, or methodological perspectives" he is working from. To enhance the validity of research findings, one needs to use multiple methods, data sources, and in the best case even multiple researchers.[24] Since triangulation is one of the main approaches being followed to highlight the trustworthiness of my research, I devoted an own section to it which I would like to refer to for further information (see section A.1.1).

The second method, is the process of member checks. Guba calls it *"the single most important action inquirers can take, for it goes to the heart of the credibility criterion"*. Doing member checks means that inquirers present their insights to other members of the same (or a similar) group that the results were derived from. Out of all insights I gained, I always wrote those down as a preparation for the next interview that might have been relevant because the new interviewee had a similar background as the one I originally gained the insights from. After talking about the particular issues, without referring to my former insights, I presented the answers of my former interviewees so that the current interviewee could challenge them. Whenever the answers were in conflict, which hardly ever happened, I scrutinized this particular aspect in the upcoming interviews.

Persistent Observation, the third method, helps identifying *"pervasive qualities as well as atypical characteristics"*.[25] This is achieved by spending sufficient time in the environment that is described. I followed this method by conducting all problem-centered interviews in China during a period of 7 months. By talking to almost 40 interviewees, I based my research on a number of participants which is unusually large for qualitative research. Many

---

[24] See Mathison (1988, p. 13)
[25] See Guba (1981, p. 85)

insights were also gained during the two years that I lived in China before starting my thesis. Even though I could not spend much time at each site that my interviewees' worked at, when the results of an interview seemed to be inconsistent with insights from other sources, I tried to understand those discrepancies by interviewing another employee of the same firm.

A fourth method for establishing credible research results is *peer debriefing*. Peer debriefing helps the researcher to detach himself from the current research problem and to reflect his latest ideas. When I was conducting the interviews, I met with colleagues at Shanghai Jiao Tong University to talk about my insights. Furthermore, I presented my insights to professionals working in China, who gave important advice by reflecting my ideas with their insights. Most meaningful were various meetings and discussion with my supervisor, Prof. Dr. iur. Bernd Lutterbeck, and my colleagues Frank Pallas, Matthias Bärwolff, Kei Ishii and Kai Dietrich.[26] I also gave lectures about my preliminary findings so that students and colleagues at my university's *Information Security Management* research group could challenge my assumptions and supported the debriefing process.

The last step to achieve credibility, *establishing referential adequacy*, was made by collecting and reviewing laws, studies, articles etc. during the entire research period – sometimes even provided by the interviewees themselves. The collected material was afterwards also used to triangulate the research results.

Transferability

For achieving context-relevant results, Guba proposes two major methods: *Theoretical/Purposive Sampling* and *Collecting a lot of Data*.

Theoretical/purposive sampling means maximizing the range of information uncovered. *"The nature of the sampling process is governed by emergent insights about what is important and relevant."*[27] I followed this approach by talking to various different stakeholders. I not only focused on companies outsourcing their IT services in China or IT outsourcing service providers but also talked to security professionals, lawyers, auditors and researchers. My interviewees held different positions, ranging from CEOs to technical administrators. Whenever I uncovered new insights that had not been mentioned before, I tried to find new interviewees in the field necessary to provide me with deeper insights or deepened my understanding by reviewing research literature and studies.

The second approach, *collecting a lot of data*, means talking to many different stakeholders but also collecting data about their backgrounds. Therefore,

---

[26] I explicitly would like to thank those people again – the team at our chair *Computers & Society*. Without their enduring support, their broad knowledge and blunt feedback, but also their personal motivation and inspiration, this thesis would not have been possible.

[27] See Guba (1981, p. 86)

each interview started and ended in a very informal manner, talking about myself and the interviewee's background – his or her current and former positions, intercultural encounters, personal background etc. Thereby, I could understand the context of the answers provided.

Dependability

Stable results can be achieved by applying three different methods: *Overlap Methods*, *Stepwise Replication* and *Audit Trails*.

Using *overlapping methods* is a form of triangulation. Multiple methods are applied for gaining insights. However, they are not only used as cross-checks but also complement each other, generating new ideas and offering new insights. How I applied this method is described in section A.1.1, focusing on triangulation and crystallization.

Stepwise replication normally means having two researchers or two separate groups of researchers comparing their results after independently analyzing the data or even independent data collection. This is one of the few methods I could not fully apply. Since I conducted all interviews on my own, there was no other researcher I could compare my results with. However, I did compare my results with scientific literature and studies in the various fields, primarily focusing on cultural studies, outsourcing and information security. I thereby generated independent results that could be verified.

The last aspect, generating *audit trails*, was followed in a way that is proposed by the grounded theory research paradigm. For various reasons, I did neither record nor transcribe the interviews.[28] However, I took handwritten notes that I could repeatedly review while writing this thesis. The grounded theory paradigm proposes this method because insights change and one needs to adapt the questions being addressed to the interviewees to the situation, the interviewees' backgrounds and the current focus of interest. Thereby, recordings and transcriptions are unnecessary. In case of arguments about the stability of results, one could still refer to the handwritten notes which represent the audit trail.

Confirmability

Confirmability of research results seems to be highly related to the other criteria of trustworthiness. Thereby, the methods being applied to underline the confirmability are similar to those of other criteria: *Triangulation*, *Practicing Reflexivity* and *Confirmability Audits*.

Triangulation, the use of multiple methods and data sources, is again the primary approach. Therefore, I would like to repeat my previous remark: Since triangulation is the most important strategy for assuring the trustworthiness of results and because it can be regarded as relevant for all four criteria, I

---

[28] For more information why I could not record the interviews, see my description of the data collection method, sections A.2 and A.3.

will address this method, and how I applied it during this thesis, in the next section.

Practicing reflexivity and conducting *confirmability audits* are the other two methods that can be applied for showing confirmability of research results. Since I discussed my research ideas with my colleagues during all phases of conducting research and writing my thesis, they reflected my approach but also my personal assumptions. I formulated and thereby codified some of my epistemological assumptions in a special section on the personal bias of my research (see section A.4). A confirmability audit can be made in the same way as the dependability audit (see above).

While conducting my research and during the entire process of writing my thesis, I had the four criteria of trustworthiness in mind. I addressed each of those criteria by using the methods described by Guba in his paper *Criteria for Assessing the Trustworthiness of Naturalistic Inquiries*. I am therefore certain and hope that I convinced the reader of the trustworthiness of my inquiry. I devoted the next section to deepening the insights on my usage of the most relevant method for achieving this trustworthiness: *Triangulation*

Credibility and Validity through Triangulation and Crystallization

As outlined above, in order to increase the credibility and validity of my work, I employ a concept very popular in qualitative research: *Triangulation*

Triangulation is *"the combination of multiple methodological practices, empirical materials, perspectives, and observers in a single study"*.[29] It not only means combining several qualitative methods, *"but it also means combining qualitative and quantitative methods"*.[30,31] Thereby, researchers can examine their research question from various different perspectives.

Researchers using triangulation as their research approach acknowledge that *"objective reality can never be captured"*. Phenomena can only be viewed and understood from a certain perspective. By basing their research on multiple research methods, researchers gain a deeper understanding of the phenomenon in question. Furthermore, they hedge against the risk of misinterpreting data by deriving their insights from different sources.

Richardson and St. Pierre argue that triangulation restricts itself to only a few perspectives and that crystallization would be the more appropriate imaginary for 'validity' of research, postmodernist texts in their case. They

---

[29] See Denzin and Lincoln (2005a, p. 3)

[30] See Flick (2006, p. 37)

[31] Todd D. Jick describes the triangulation paradigm and researchers working in the field as sharing *"the conception that qualitative and quantitative methods should be viewed as complementary rather than as rival camps. In fact, most textbooks underscore the desirability of mixing methods given the strengths and weaknesses found in single method designs."* See Jick (1979, p. 602), also published in Van Maanen (1983)

see the triangle as a two-dimensional object which is fixed and which helps discovering the coordinates of a point, or an object, that is at a fixed location and therefore can be triangulated. The crystal, in contrast, *"combines symmetry and substance with an infinite variety of shapes, substances, and angles of approach. Crystals grow, change, and are altered, but they are not amorphous. Crystals are prisms that reflect externalities and refract within themselves, creating different colors, patterns, and arrays casting off in different directions. What we see depends on our angle of repose — not triangulation but rather crystallization."*[32]

I agree with them that there is no single truth that can be triangulated but there is something, which can be seen as our present truth, that we can get closer to and understand more thoroughly. This present truth is not fixed and we need to employ more sources and question our assumption in order to realize whether we are moving in the right direction or if we should adjust our strategy due to new insights.

This leads us to another concept that is very important for understanding my research approach, the *hermeneutic circle.*

A.1.2 The Hermeneutic Circle

Every time a researcher enters a new field, he needs to think about the context he is conducting his research in. He is well-advised to question traditional assumptions but also his own ones. He must be open to learn and to integrate his new insights into his own research. He might be proved wrong or might himself realize that he is on a track that seemed to be promising but is leading into the wrong direction. The researcher might even be heading into the right way but stumbles upon methods that seem to be more effective of efficient. If that happens, he should reconsider his research strategy and insights that he gained up to now and adapt to his new learnings. This process of always challenging the status quo, scrutinizing why something is done in a certain way and adapting to new insights is probably one of the core drivers for scientific and social progress. It can be called the *hermeneutic circle.*

The word *hermeneutics* is often said to go back to the Greek god Hermes. One of his tasks was to deliver messages of the gods to the humans. To fulfill this task, *"Hermes translated the divine idiom into human speech and thus became [...] the emblem of the task of translation between different orders, times and places."*[33] Aristotle used hermeneutics, or rather the Greek words *Peri Hermeneias*, as the title of a work on the interpretation of language and logic.[34]

---

[32] See Richardson and Pierre (2005, p. 963)

[33] See Goodrich (1998, p. 506), published in Craig (1998)

[34] His work is today still available under its English name *On Interpretation* or its Latin title *De Interpretatione.*

"Hermeneutics [traditionally] is an approach to the analysis of texts that stresses how prior understandings and prejudices shape the interpretive process."[35]

It has long been seen as the theological principles of exegesis. Theologians used hermeneutics as an approach to analyze the bible and to search for the meaning of the written words. Hermeneutics stresses the distinction between the letter and the spirit of the text.[36] It thereby promotes the idea that context matters. The spirit of a text, as it has been written centuries ago, can only be interpreted with the appropriate knowledge about the earlier period. Not only the point in time matters but anyone interpreting texts needs to understand cultural and sociological circumstances that influenced the author and his style of writing.

Even though hermeneutics has been a prominent concept in biblical exegesis, it gained new momentum with the protestant reformation, starting with Martin Luther at the beginning of the 16th century. For the reformation of the catholic church, protestant theologians also based their ideas on the same source as their catholic counterparts. The interpretation of the bible and its spirit turned into a core argument. It was not until German theologian Friedrich Daniel Ernst Schleiermacher that hermeneutics opened to a broader audience. He challenged the assumption that hermeneutics can only be applied to scriptural texts and rather saw it as a generic method for the interpretation of text and language.[37] He often compares hermeneutics to the way children acquire language.[38]

This comparison helps understanding the use of a new term, the *hermeneutic spiral*. Researchers preferring this term over *hermeneutic circle* argue that a circle is the wrong image of hermeneutics. When interpreting texts, one does never come back to the starting point, instead raising to a new level of understanding. This *"hermeneutic spiral is endless."*[39] One does never reach an end because rereading, thinking, discussing always leads to new insights that influence the interpretation of the text. Also other seemingly unrelated events change a researcher's thinking so that reading a text after a few years is likely to lead to another, hopefully more insightful, interpretation.

---

[35] See Denzin and Lincoln (2005a, p. 27)

[36] There is a similar argument in legal contexts, which made hermeneutics an important method in this field as well. Legal scholars argue about the letter of the law and the spirit of the law. The interpretation of a law's spirit is especially controversial when the written text has already been produced generations ago. Constitutions are therefore viewed from various perspectives. The importance of legal or judicial hermeneutics is obvious following ongoing debates about the role of the state for providing national security or the future of copyright.

[37] See, for example, *The Significance of Schleiermacher's Project of a General Hermeneutics* Palmer (1969, p. 94 ff.)

[38] See Schleiermacher (1998, p. xi)

[39] See Hart (2000, p. 218)

Hermeneutic spiral is also the appropriate term for the paradigm this thesis is following. With this research, I do enter a new field, combining information security research with social sciences, cultural studies in particular. Therefore, I enter the spiral at the bottom and all I can do is to make a few turns, get closer to what I called before, the present truth. For reaching another level of understanding, I applied a couple of different methods, being described in various other sections of this thesis. I also take on different cultural perspectives to gain insight from other points of view.

In order to understand why I am talking about hermeneutics, we need to take a look at how hermeneutics developed after Schleiermacher.

Today, hermeneutics is not limited to the interpretation of texts anymore. One of the first researchers and strong supporters of Schleiermacher was German philosopher Wilhelm Dilthey.[40] Dilthey argued that hermeneutics should be broadened to all aspects of life.[41] Not only texts but also human behavior, laws, art, architecture etc. can only be understood by interpreting them in the context of their appearance. To understand a particular culture, one should always shift between specific behavior of individuals and an image of the culture as a whole. Thereby, one's understanding of the culture is spinning upwards in the hermeneutic spiral. But this explanation of the process also shows why the hermeneutic spiral is endless. If one's understanding of a culture changes every time we look at an individual person, the point of view from which we interpret the next individual's behavior is never constant. When we do research, we enter a recursive process.

After Schleiermacher and Dilthey opened hermeneutics to other applications than the sole interpretation of texts, it has been adopted as a research paradigm by various disciplines, including computer science.

Terry Winograd, is one of the strong advocates of bringing hermeneutical research into the field of computer science, artificial intelligence in his case. In *Understanding Computers and Cognition: A New Foundation for Design*, which he authored with Fernando Flores, he argues that designers, or rather architects, of computer systems operate in a mental frame that they can not escape. Thereby, architects are restricted in their view how computers should operate, which functions they can and cannot fulfill – what computers are. To fully unfold the full potential of computer systems, they need to be developed by people who manage to break out the frame.

In their words, the key to understanding their work, the design of computer systems and the mental frame *"lies in recognizing the fundamental importance of the shift from an individual-centered conception of understanding to one that is socially based. Knowledge and understanding (in both the cognitive and linguistic senses) do not result from formal operations on mental*

---

[40] See, for example, Dilthey (1972)

[41] Other researchers, partly criticizing Dilthey but nevertheless following his general ideas, include prominent researchers and philosophers like Heidegger, Gadamer and Habermas.

representations of an objectively existing world. Rather, they arise from the individual's committed participation in mutually oriented patterns of behavior that are embedded in a socially shared background of concerns, actions, and beliefs."[42] People *"cannot be impartial, detached observers of the world in which they live, but they must decide and act using heuristics which they have as part of their effective histories."*[43]

In summary, hermeneutics should rather be called a paradigm than a method. It can be seen as a mental framework that unifies a group of researchers, gaining insights by integrating the context of research objects into their understanding – always questioning what they thought before.[44] Thereby, they work recursively, gaining insights by moving upwards in a spiral of understanding.

Researchers who work hermeneutically accept the fact that their interpretation of texts, dialogues and experiences are biased. Their interpretation is not only influenced by their national culture (Chinese, German, U.S. American etc.), the social setting they grew up in, but also by the experiences that they have made later in their lives. It is also based on small factors like the books they read, movies they have seen, discussions they have had with friends, colleagues etc. It certainly differs according to the century, decade etc. researchers live and work in.[45]

A.1.3 Grounded Theory

Researchers in favor of the hermeneutic research paradigm tend to apply qualitative research methods. They use these methods by iterating through various cycles as long as they have not gained the insights they were looking for and as long as their understanding of the research problem still changes considerably in every cycle. The research methodology that seems to be most consistent with this research paradigm is called *grounded theory* (GT). This thesis follows a research strategy that is inspired by but not fully consistent with the grounded theory approach. It abides the general research principles defined for grounded theory, but does not make use of strict data analysis methods because it is mainly explorative in nature.

Grounded theory is a research strategy that was developed by American sociologists Barney G. Glaser and Anselm L. Strauss. In 1960, they started working on a sociological study in the medical field. Their goal was to understand how people handle death and interact with dying patients – primarily focusing on different aspects of awareness in the process of dying. Five years later, they published a book about their findings, *Awareness of Dying*.[46] They

---

[42] See Winograd and Flores (1986, p. 78)

[43] See Mallery, Hurwitz, and Duffy (1986, p. 21)

[44] See Gadamer (2004)

[45] The impact that my personal bias has on the results of this thesis, is explained in section A.4.

[46] See Glaser and Strauss (1965)

based their insights on a large amount of data they had collected in previous years in various hospitals. They did not have any pre-formulated hypothesis and the situation they witnessed was different in every setting. Therefore, they decided to develop their own research methodology, which they later called *grounded theory* and first described in their 1967 book *The Discovery of Grounded Theory: Strategies for Qualitative Research*.[47],[48]

Even though the word *qualitative* is part of the book's name, grounded theory is not necessarily only based on qualitative data. Its main idea is the generation of a theory from collected data[49] – *the theory is [thereby] grounded in the data*.[50] Grounded theory is neither solely inductive nor deductive in nature but rather combines both processes of reasoning. The formulation of a hypothesis happens on the basis of qualitative but also sometimes quantitative data. This hypothesis is thereafter mapped with theories and again verified in a deductive manner by comparing it to other empirical material.[51]

Appropriate Data for Grounded Theory

Since grounded theory is totally based on data, it is important to define what can be considered as adequate data. I would like to highlight three text passages by Glaser and Strauss in which they provide their definition of data that can be used for grounded theory:

Glaser and Strauss, 1967

In their prime monograph on grounded theory, Glaser and Strauss use the term *slices of data*. They say that *"[d]ifferent kinds of data give the analyst different views or vantage points from which to understand a category and to develop its properties"*.[52] They call it slices of data because they believe that each data source can only provide a limited view on the research issue which is observed. Researchers can only gain holistic insights when looking at a problem from different perspectives and by combining data from various sources. Glaser and Strauss thereby see those slices of data as important for gaining a holistic picture but at the same time also support triangulation as an important research paradigm.[53]

Strauss, 1987

In his 1987 book *Qualitative Analysis for Social Scientists* Anselm L.

---

[47] See Glaser and Strauss (2006), first published in 1967

[48] Glaser and Strauss later argued about the specific definition and the way grounded theory should be conducted. However, their argument does not influence the inspiration gained from both researchers and is therefore not particularly highlighted in this thesis.

[49] See, for example, Glaser and Strauss (2006)

[50] See Salinger, Plonka, and Prechelt (2008, p. 11)

[51] See, for example, Glaser (1978, 1998, 2002b)

[52] See Glaser and Strauss (2006, p. 65 ff.)

[53] See also Locke (2001, p. 45)

Strauss particularly mentions experiential data and personal experiences as highly valuable. "[He] refers to experiential data as 'experiences of various kinds' and mentions also personal experiences as 'potential gold'."[54] He therefore underlines the importance of qualitative data for theory generation.

Glaser, 2001

The third and most concise quote, is by Barney G. Glaser. *"'All is data' is a well known Glaser dictum. What does it mean? It means exactly what is going on in the research scene is the data, whatever the source, whether interview, observations, documents, in whatever combination. It is not only what is being told, how it is being told and the conditions of its being told, but also all the data surrounding what is being told. It means what is going on must be figured out exactly what it is to be used for, that is conceptualization, not for accurate description. Data is always as good as far as it goes, and there is always more data to keep correcting the categories with more relevant properties."*[55]

All is data sums up the discussion of adequate data for doing grounded theory pretty well. Data can be anything: informal interview notes, research studies, expert group meetings, newspaper articles, blog posts, personal conversations, quantitative data like statistics etc.

Rules for Doing Grounded Theory

Barney G. Glaser often advocates that the researcher should have as much freedom and a clear mind when conducting research. In order to achieve best results, there are two rules that I followed during each step of writing this thesis: *No Pre-research Hypothesis* and *No Taping and no Transcriptions.*

No Pre-research Hypothesis

Grounded theory is an emergent process in which theories emerge out of the data which has been collected. It is highly explorative in nature. If researchers would conduct a profound literature review and formulate a hypothesis before starting data collection, their research would exhibit preconceptions and assumptions that might be misleading. In order to work with as little bias as possible, I consulted most literature – and there was not much – while and after conducting the interviews in China. Thereby, I could triangulate my findings and generate insights without pre-research assumptions.[56]

---

[54] See Marschan-Piekkari and Welch (2004, p. 158), referring to Strauss (1987, p. 10–11)

[55] See Glaser (2001, p. 145), as cited in Marschan-Piekkari and Welch (2004, p. 158), or Glaser (2002a)

[56] See, for example, *The Constant Comparative Method of Qualitative Analysis* Glaser and Strauss (2006, p. 101–115)

No Taping and no Transcriptions

Taping and transcriptions of interviews are very common in qualitative research. However, qualitative researchers often restrain from using those techniques, rather jotting down hand-written notes during interviews. In their opinion, tape-recording and extensive note-taking are distracting and unnecessary.[57] Insights and the research direction change with every interview and interviewees ideally have different backgrounds. Research results do not rely on every word the interviewees' expressed but rather on the big picture, generated from the accumulation of all data. Those reasons were part of my decision neither to tape nor to fully transcribe the interviews I conducted. Moreover, there was one other major reason, concerning the openness of the interviewees when being tape-recorded, that I will describe in sections A.2 and A.3. However, I did take notes during the interviews for my own review of the content of the interview and as an audit trail.[58]

Criteria and Goals of Grounded Theory

Since insights are gained inductively when doing grounded theory, GT researchers follow the approach that *"the theory should fit the data"*. This is one of the large differences to traditional research (usually based on quantitative data) in which *"the data should fit the theory"*.[59] The main flaws of the second approach are that *"data can be forced to fit the theory"* and even if no data has been found that supports the theory, it is not the fault of the theory and it can still be regarded as valid.[60] Those problem are avoided when doing grounded theory, since there is no theory without any data.

Theories derived following the grounded theory approach exhibit the following properties or follow the following four goals:[61] *Fit, Modifiability, Relevance* and *Workability*.

The theory *fits* the data and when more data is collected that is not in line with the preliminary theory, the theory needs to be adapted. This directly leads to the second criteria, the theory needs to be *modifiable*. It can not be static because it does not represent a fact but rather an image of the current understanding of the problem. However modifiable a theory might be and however well it fits the data, it is useless when it does not have any *relevance* for the real world and provides a *workable* understanding of it. Researchers should always ask themselves why they work on their theory and what kind of problem it solves besides satisfying a purely academic interest.

Glaser himself expresses those criteria in the following way: *"GT is inducted from systematically collected facts, which in the process for generating*

---

[57] See, for example, Dan Goodley and Moore (2004, p. 119)

[58] For information on the importance of an audit trail, see section A.1.1.

[59] See Glaser and Strauss (2006, p. 261)

[60] See Glaser and Strauss (2006, p. 261)

[61] See, for example, Charmaz (2005, p. 527)

GT from data, constantly verifies its fit, relevance and workability, and adjusts (modifies the concepts and their relationships) the theory to the facts to achieve fit, relevance and workability."[62]

Kathy Charmaz, Professor of Sociology at Sonoma State University, would like to reopen the debate about criteria for grounded theory studies in her article *Grounded Theory in the 21st Century*. She proposes four criteria which she calls *credibility, originality, resonance* and *usefulness*.[63] Scrutinizing her definitions, one sees that her criteria exhibit similarities to Glaser's criteria – especially her criteria resonance and usefulness. Credibility and originality seem to be rather new but credibility is achieved by the sticking to the process behind grounded theory (basing insights on various sources) and originality is linked to Glaser's criterion relevance.

Throughout the entire thesis, I repeatedly show how I conducted my research with the criteria and goals of grounded theory – the traditional ones by Glaser and the new ones by Charmaz – in mind.

Closing Remarks

My research strategy is inspired by but not fully consistent with grounded theory. I followed grounded theory's most fundamental idea, the generation of insights on the basis of data – whereas data can be anything, qualitative and quantitative alike. Furthermore, I stuck to the basic rules of grounded theory, no formulation of pre-research hypothesis and no tape-recording or transcribing. Thereby, my insights fit the data and the real world, my concepts are modifiable, workable and relevant. Their credibility is underlined by abiding Guba's criteria, defined in section A.1.1 on trustworthiness.

A.2 Problem-centered Interviews

In the previous sections, I already described the research philosophy (hermeneutics), the research strategy (grounded theory) and talked about the trustworthiness of qualitative research (triangulation). What I have not written about in detail yet is the data collection method that I used to gain my insights and base my research on. I primarily used semi-structured interviews that I conducted in China. I will talk about the interview method itself in this section. In the next section, I will describe my interview setting and the target group I interviewed.

Many researchers try to understand information security by distributing questionnaires to companies and evaluating the figures afterwards. This is a valid approach if one is interested in statistical data (How many companies use virus scanners with up-to-date virus definitions?, How do companies rate

---

[62] See Glaser (2004)

[63] See Charmaz (2005, p. 528)

the influence of SOX[64] on their IT security spending on a scale from 1 to 5?, etc.). However, as mentioned in earlier sections, in order to plunge more deeply into an organization and to analyze human behavior and the reasons behind it, quantitative approaches do not work and qualitative research is necessary.[65]

Therefore, data should rather be prosaic – or better narrative – than close-ended or short-answered.[66] The data collection method that the research results of this thesis are based on reflects this insight.

Interviewing is the art of asking questions and getting answers.[67] *"[It] is one of the most common and powerful ways in which we try to understand our fellow humans. Interviewing includes a wide variety of forms and a multiplicity of uses. The most common form of interviewing involves individual, face-to-face verbal interchange, but interviewing can also take the form of face-to-face group interchange and telephone surveys."*[68] Qualitative expert interviews are an important method that is normally used in social research but is gaining popularity among engineers and economic researchers recently. It can be seen as the most important data collection method for *narrative inquiries*, a particular type of qualitative inquiries.[69]

I did choose qualitative expert interviews as my primary data collection method and combined as well as cross-checked the results with data from other sources.[70]

As mentioned above, those interviews can be conducted in various ways. Since I addressed highly sensible issues, talking about information security concerns and incidents, I decided to conduct the interviews in an individual, face-to-face verbal interchange. Group sessions and a conversation via telephone would have constrained me in building up a personal relationship with the interviewee which was crucial for an open discussion. For further information on the need of building up this relationship and how to create the appropriate atmosphere, I would like to refer to the next section (A.3).

Even after narrowing the group of possible interview techniques down to those appropriate for qualitative inquiries in a one-on-one setting, there still are different ways of conducting the interview itself. Andreas Witzel developed

---

[64] SOX stands for Sarbanes Oxley Act, an US-American law whose goal is to combat fraud, improve reliability of financial reporting and restore investor confidence. See Wagner and Dittmar (2006)

[65] See Kromrey (2005, p. 4 ff.) and see section A.1.1

[66] See Chase (2005, p 651)

[67] See Denzin and Lincoln (2005b, p. 643): *"The interview is a conversation — the art of asking questions and listening. It is not a neutral tool, for at least two people create the reality of the interview situation."* For deeper insights into the bias in conducting and analyzing interviews, see section A.4.

[68] See Fontana and Frey (2005, p. 697 f.)

[69] See Chase (2005)

[70] See section A.1.1 on *triangulation*

a method belonging to this group, called the *problem-centered interview*.[71] It is centered around a specific topic or problem and scrutinizes the interviewees experiences, perception and reflexion of the core issues.

As opposed to quantitative methods, the problem centered interview does not require a codified list of questions but uses a guideline that helps the interviewer to navigate through the dialogue. It is just meant as a support for the interviewer and is not shown to the interviewee. When the interviewer gained some experience, he memorizes the guideline as a path in his mind so that he does not rely on the printout anymore. The goal is to get the interviewee into a state of storytelling and leading him on the paths one wants to analyze. As opposed to the narrative interview, the problem-centered interview does not have a clear distinction between phases for narration and questioning which makes it possible to lead the interviewee. It is important to bring the person who is being interviewed into a state of narration in which he addresses most of the interviewer questions (or better covers all topics of interest) but not necessarily in any particular order. This enables the interviewer to gain insights into experiences, feelings and ideas through personal stories told by the interviewee. A focus, further isolating the already focused (centered) problem, can be set by asking specific questions.

This communication strategy can be divided into four central strategies: *the conversational entry*, *general* and *specific prompting*, and *ad hoc questions*[72]

Each of these strategies can and should be used during the interview. As a rule of thumb, they should be applied in this particular order: Finding a conversational entry and later on asking general and more specific questions. When a topic particularly arouses the interest of the interviewer or something needs to be clarified, ad hoc questions are an appropriate inquiry method. However, this order should not be seen as a strict frame, of course, there can be loops within the communication strategy and especially ad hoc questions can be asked in every step of the interviews. Nevertheless, the interviewer should try to maintain the narrative state of the interviewee and not interfere too much with the his or her story-telling.

If used in a skilled manner by an experienced interviewer, the application of the problem-centered interview method allows the interviewer to analyze highly sensible topics, which normally cannot be openly addressed.[73] The interviewee might not even be aware of some circumstances that become visible by talking about it.

Since topics like information security in a company, problems with superiors or criticism at the state are highly sensible issues, the problem-centered interview was the most promising method for analyzing information security issues in outsourcing relationships in China.

---

[71] See Witzel (1982), Witzel (1989, p. 227 ff.), Witzel (1996, p. 49 ff.), Witzel (2000)
[72] See Flick (2006, p. 161)
[73] See also section A.3

A.3 Conducting Problem-centered Interviews in China

I believe that one needs to fully immerse into a setting – be it social, economic, cultural, etc. – in order to understand it. Taking on this stance, I knew I had to live and work in China in order to grasp the information security incidents that occur there and to analyze which of those are culture-related.

Therefore, after having lived in Shanghai already from summer 2003 until spring 2005 and in autumn 2005, I moved to China again in 2006. I gave guest talks at Shanghai Jiao Tong University and did research for my thesis from August to December 2006. During this time, I conducted 38 qualitative interviews with professionals with diverse backgrounds – business-wise but also regarding their personal background (origin, education, etc.).[74] I talked to outsourcing providers, companies that outsource their IT infrastructure, security professionals, law firms as well as external auditors operating in China. A distribution of the backgrounds of my interviewees is presented as figure A.2.

Fig. A.2. Backgrounds of Interviewees

---

[74] Without the help of many friends and business partners in Shanghai, I would never have managed to reach such a high number of respondents. I owe a great deal especially to Joerg Heil, general manager at hartung:consult Shanghai, one of the first – if not literally the first – local SAP partners (service provider and consultancy) in China. He tremendously supported my search for interviewees by offering me access to his entire web of business contacts and even personally establishing some contacts himself. Also Paul Blome and others at the German Chamber of Commerce in Shanghai were highly supportive by granting me access to their network. Their support was crucial for writing this thesis.

As shown in the chart, outsourcing providers, their clients and security professionals made up the biggest share of respondents. By talking to outsourcing providers, I could analyze how they approach and manage information security, how they deal with security incidents and how they interact with clients. Their clients could talk about their view of the outsourcing relationship and how they tried to minimize security risks and to reduce information asymmetries. External security professionals could describe their view of information security risks in China and talk about issues they saw and hopefully solved at their clients' sites. This already generated a rather holistic view on security risks in outsourcing partnerships. However, those interviews raised other questions that made it necessary to broaden the group of interviewees and talk to lawyers and auditors who could provide another external view on particular aspects of those outsourcing relationships. In others, I subsumed researchers I talked to and a few other interviewees who did not fit any other category.

Interviewing people with diverse backgrounds and not focusing on one group of respondents is highly important following the principles of grounded theory. If one gains insights into a field, one should follow the lead and talk to others who might be able to provide further knowledge. Furthermore, researchers should try to view a problem from as many perspectives as possible. By analyzing the problem from different perspectives, one can gain a more holistic understanding of the issues and its context. This leads to the another reason for interviewing a diverse group of people – the trustworthiness of an inquiry. As mentioned earlier, to increase the trustworthiness, triangulation is a highly acknowledged method.[75] This does not only mean applying different research methods but also combining data from various sources – quantitative and qualitative alike. This also includes a diversification of perspectives by talking to people with different background. Thereby, I could cross-check if and how the same problem has been described from the outsourcing provider's and its client's view.

Conducting the interviews in China, I realized how important the choice of the data collection method and the interview setting are. Especially the interview atmosphere played a pivotal role. The more informal the atmosphere, the more honest and open the answers of the interviewees. When talking in offices, especially with other colleagues in the same room (which happened seldom), the respondents were rather reserved. I assume that they were afraid of disclosing security and also publicity relevant information and thereby tried to restrict their answers to those that highlighted the professionalism of their firm. In these settings, they also preferred answering specific questions rather than talking freely about their view. Some interviewees seemed not to talk with their own voice, expressing their own opinion, but tried to resort to corporately correct answers. Thereby, conducting the interviews in a problem-centered manner and using a few psychological 'tricks', which I will talk about later, could change the atmosphere which turned out to be highly beneficial.

---

[75] See section A.1.1

In order to get interviewees to talk about security issues openly and thereby disclose seemingly sensible information, there were two important preconditions: *Trust* and *Familiarity and Spontaneity*.

Trust

There needs to be a bond between the interviewer and the interviewee. The interviewee must trust the interviewer that results are only presented anonymously and no information is spread to clients or competitors. Therefore, building up a personal relationship is crucial.

Familiarity and Spontaneity

The interviewee should forget that he or she is being interviewed. The interview should rather feel like an interesting chat than a formal process of answering predefined questions. Questions addressed to the interviewee should always relate to what was said before. It should seem like the interviewer is asking those questions just because he is personally interested in what was said and would like to deepen his understanding for personal and not necessarily for academic reasons. The interview should feel like a chat rather than a formal interview.

In order to create trust and a familiarity that enabled the interviewees to talk openly about their personal view, a couple of aspects were crucial. The atmosphere of the interview setting but also the interview method – which defined how the interview was conducted – had to support a rather private talk.

To create a more informal atmosphere, I tried placing the interviews at informal locations – or at least in a one-on-one setting. I conducted the most insightful interviews at bars or restaurants. The two interviews that I appreciated most happened at Starbucks and on the roof terrace of element fresh, a lifestyle restaurant chain in Shanghai.[76]

Besides selecting a suitable location, I used other means for creating an appropriate atmosphere. When the interviews happened at offices, I brought goodies which I placed on the table and offered to the interviewee. When the interviews were arranged at restaurants or cafes, I often had coffee, cake or a proper meal together with the interviewees. This already made the setting more private. I tried further supporting this atmosphere by starting the talk with an informal chat about ourselves, current issues like events, art, common acquaintances, etc. – all unrelated to the topic which was about to be discussed. This was easier, or possible at all, because many of the interviewees were friends or business contacts of people I had talked to before. Thereby, we almost always had a starting point for our conversation.

---

[76] Of course, those interviews were conducted at times and spots within the restaurants in which only very few other customers were around. Otherwise, the noise level but also the pure presence of other visitors would have destroyed the atmosphere and thereby the interview setting.

Conducting the interviews in a problem-centered way enabled me to lead through the interview by deepening on issues the interviewee addressed and to bring up topics that I was interested in without asking closed questions. During the first interviews, I placed my semi-structured questionnaire on the table to check if I had addressed every field I was interested in. After conducting a few interviews, I did not need the guideline anymore because I had internalized the questions. This made the atmosphere even more relaxed. I managed to put most interviewees into a state of story-telling (narrative state) in which they presumably forgot that an interview is being conducted. By leading the interview instead of asking closed questions, I tried to perpetuate this state for as long as possible. For bringing the interviewees into this state it was furthermore highly important to stick to rules presented in section A.1.3: *No Pre-research Hypothesis*, *no Taping* and *no Transcriptions*

If a hypothesis had been formulated before the first interview, my mind would have been framed and the questions I would have asked had limited the horizon of the answers as well. Verifying a hypothesis by asking closed questions would have been counterproductive for exploring the field of culture-related security issues. A few years ago, I already conducted interviews for my diploma thesis. I tried taping the entire interview so that I could review it afterwards but soon realized that the interviewees responded in a very different manner when the interview was taped. I assume that some respondents would forget the tape after a while but others rather present a different view, not their personal opinion, when they are afraid that they disclose sensible information. Having it recorded adds another barrier for talking about information security openly. For my diploma thesis, I soon dismissed recording the interview and resorted to handwritten notes. For this thesis, I made use of the experiences I gained and followed grounded theory rules from the start. I dismissed techniques that are unnecessary and even counterproductive – tape-recording and transcribing the interviews in particular – and focused on generating a productive but informal atmosphere so that the interviewees talked about their experiences and knowledge without being framed by corporate rules or their fear of disclosing sensible information. Handwritten notes that I made during and after the interviews enabled me to remember the content of the interview even after a couple of months.

The results of the interviews – which are private and professional experiences, insights and stories of the interviewees – enabled me to analyze China-specific security problems. Many of those security risks were culture-related, but also legal, institutional and technological aspects played an important role.

A.4 Personal Bias

I am fully aware that the decisions how to conduct my research, how to structure this thesis and how to present the results to readers – even that fact that

I chose this particular topic for my thesis – are all subject to a personal bias. Even though I lived in China for three years and spent a big share of my time in the past years reading about cultural differences, and the Chinese culture in particular, I still grew up in Berlin, Germany, and lived there for most of my life.

Since I, myself, after having spend quite some time in Asia, feel more like a European than a German, I assume my bias might be called a European one. If we look at the dimensions that are analyzed in this thesis, we will notice that European countries – although being widely distributed over the spectrum[77] – tend to occupy places (or values) on the middle of the dimensional scales. I hope that I can make use of this advantage, not belonging to one of the cultures on the extremes, and describe cultural differences and their impact on information security in a largely "objective" matter.

I have presented and discussed my results with many international friends and colleagues and hope that this made my work more applicable and understandable from other cultural perspectives. However, this thesis will always have a bias that is not German, or European, but solely my personal one – reflecting my education and my environment – my personal experiences. Already the data collection method – conducting qualitative expert interviews – exhibits a personal bias. Denzin and Lincoln write the following about its bias: *"This method is influenced by the personal characteristics of the interviewer, including race, class, ethnicity, and gender."* [78] Andrea Fontana and James H. Frey add in an article on the history of conducting and analyzing interviews: *"[Interviewing] is inextricably and unavoidably historically, politically, and contextually bound."*[79]

This is neither a flaw of the methodology that is applied to gather and analyze research results nor of the way they are presented. Furthermore, a personal bias is not even limited to qualitative research. The selection and formulation of questions being asked, the way in which those questions are addressed to respondents as well as the way they are analyzed, interpreted and presented to the reader are never value free and always reflect the author's personal background. Thinking in broader terms, even the decision to focus on a certain research topic is based of personal experiences and beliefs.

The fact that research can not be detached from the authors personality does neither derogate the insight that research offers nor limit the influence

---

[77] There are vast differences between Northern and Southern, Eastern and Western European cultures. But even German culture is not always the same as French. Germany, for example, has a universalist (rule-based) society, whereas French are better described as particularists (relationship-based). (See 5.5.6) And to plunge even deeper into single societies, people living in Berlin have a largely different *mental programming* than Munich residents, children from Steglitz-Zehlendorf (a quarter in the South-West of Berlin) grow up in another culture than their fellow Berliners in Marzahn (a quarter in North-East Berlin), . . .

[78] See Denzin and Lincoln (2005b, p. 643)

[79] See Fontana and Frey (2005, p. 695)

it can have on other research fields and society at large. It is only something that authors and readers need to be aware of.

A.5 Concluding Remarks

That all said, I would like to summarize all thoughts that I presented above. They include personal beliefs and a philosophy that is part of my personality. Furthermore, I chose a methodology that was most appropriate for understanding my research problem and also fit to my personal belief of how research should be done.

The entire research setting is visualized in figure A.3.

Fig. A.3. Research Setting of this Thesis

The research conducted can be labeled as *qualitative exploratory research*. The goal of this thesis is to describe the influence of culture on information security. Therefore, my research needs to open – to explore – a new field of research that has not been entered before.

The main philosophy behind the thesis is *hermeneutics*. I believe that research can only be done by understanding the context and the context can only be understood by studying individual behavior. If one observes individuals, one continuously adapts one's own mental model so that one enters a hermeneutical spiral. This spiral is endless and all we can do is to gain

new insights. In order to gain those insights, one needs to observe 'reality' without pre-formulated hypothesis. Research findings should be derived directly from experiences made and empirical data collected. *Grounded theory* was therefore my research strategy of choice – or rather inspired my research strategy. Knowledge gained inductively, by looking at individual behavior, can be formed into a theory which can itself be verified deductively by comparing it to more data again. The data collection method applied for gaining data was the *problem-centered interview*, a semi-structured interview technique developed by Andreas Witzel. In order to increase the trustworthiness of this form of research, findings were triangulated, or rather crystallized, and qualitative data was cross-checked with quantitative data like results of surveys. All findings were matched with a thorough review of existing literature.

However objective researchers try to conduct their interviews and regardless of how extensively they try to verify their findings by comparing them with other sources, research is always conducted with a personal bias that needs to be accepted as it is. Researchers only need to be aware of its existence.

B

Acronyms, Tables and Figures

Acronyms

APAC Asia-Pacific

BPO Business Process Outsourcing
BSI Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)

CIA Confidentiality, Integrity, Availability
CMMI Capability Maturity Model Integration
COBIT Control Objectives for Information and related Technology
CPC Communist Party of China
CSIA China Software Industry Association

DNS Domain Name System

EMEA Europe, the Middle East and Africa

GDP Gross Domestic Product
GT Grounded Theory

HC High-Context
HDI Human Development Index

ICAO International Civil Aviation Organization
ICT Information and Communication Technology
IDS Intrusion Detection System

IDV	Individualism
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISO/IEC JTC 1	Joint Technical Committee 1 of the International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LC	Low-Context
LTO	Long-Term Orientation
MAS	Masculinity
MECE	Mutually Exclusive and Collectively Exhaustive
NASSCOM	National Association of Software and Service Companies
NDA	Non-Disclosure Agreement
OECD	Organisation for Economic Co-operation and Development
PDI	Power Distance Index
PRC	People's Republic of China
ROC	Republic of China
ROI	Return on Investment
ROSI	Return on Security Investment
SaaS	Software as a Service
SAIC	State Administration of Industry and Commerce
SEMC	State Encryption Management Commission
SHB	Workshop on Security and Human Behaviour
SLA	Service Level Agreement
SME	Small and Medium Enterprises
SOE	State-Owned Enterprise
SOX	Sarbanes Oxley Act
SSH	Secure Shell
UAI	Uncertainty Avoidance Index

UNESCO United Nations Educational, Scientific and Cultural Organization

VPN   Virtual Private Network

WAPI   WLAN Authentication and Privacy Infrastructure

WDI   World Development Indicators

WEIS   Workshop on Economics and Information Security

WFOE   Wholly Foreign Owned Enterprise

WGI   Worldwide Governance Indicators

WTO   World Trade Organization

List of Tables

List of Figures

References

Adams, J. (1982). The efficacy of seat belt legislation: A comparative study of road accident fatality statistics from 18 countries. *Society of Automotive Engineers* (820819). Online: `http://www.sae.org/technical/papers/820819` [12.08.2007].

Adams, J. (1995). *Risk*. London: Routledge.

Adams, J. and M. Hillman (2001). The risk compensation theory and bicycle helmets. *Injury Prevention 7*, 89–91.

Adler, N. J. (1983a). Cross-Cultural Management Research: The Ostrich and the Trend. *The Academy of Management Review 8*(2), 226–232.

Adler, N. J. (1983b). A Typology of Management Studies Involving Culture. *Journal of International Business Studies 14*(2), 29–47.

Adler, N. J. (2001). *From Boston to Beijing: Managing with a World View*. Cincinnati, Ohio: Thomson Learning.

Adler, N. J. (2002). *International Dimensions of Organizational Behavior* (Fourth ed.). Cincinnati, Ohio: Thomson Learning.

Adler, N. J., R. Doktor, and S. G. Redding (1986). From the Atlantic to the Pacific Century: Cross-Cultural Management Reviewed. *Journal of Management 12*(2), 295–318.

Agyekum, K. (2004). The socio-cultural concept of face in Akan communication. *Pragmatics & Cognition 12*(1), 71–92.

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics 84*(3), 488–500.

Aljifri, H. and D. S. Navarro (2003). International Legal Aspects of Cryptography. *Computers and Security 22*(3), 196–203.

Amberg, M. and M. Wiener (2006). *IT-Offshoring. Management internationaler IT-Outsourcing-Projekte*. Heidelberg: Physica-Verlag.

Amnesty International (2008). Amnesty International Report 2008. The State of the World's Human Rights. Online: `http://thereport.amnesty.org/document/101` [14.09.2008].

Anderson, R. J. (1994a). Liability and Computer Security: Nine Principles. In: D. Gollmann (Ed.), *ESORICS*, Volume 875 of *Lecture Notes in Computer Science*, Heidelberg, pp. 231–245. Springer.

Anderson, R. J. (1994b). Why Cryptosystems Fail. *Communications of the ACM 37*(11), 32–40.

Anderson, R. J. (2001). Why Information Security is Hard – An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference. ACSAC 2001*, 358–365. Online: `http://www.acsac.org/2001/papers/110.pdf` [18.05.2006].

Anderson, R. J. (2002). Unsettling Parallels Between Security and the Environment. *Workshop on the Economics of Information Security 2002*. Online: `http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt` [02.02.2007].

Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (Second ed.). Indianapolis: Wiley.

Anderson, R. J., R. Böhme, R. Clayton, and T. Moore (2008). Security Economics and the Internal Market. *European Network and Information Security Agency (Report)*. Online: `http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf` [26.6.2008].

Anderson, R. J. and T. Moore (2006). The Economics of Information Security. *Science 314*(5799), 610–613. DOI: 10.1126/science.1130992.

Anderson, R. J. and T. Moore (2007a). The Economics of Information Security: A Survey and Open Questions. Conference on the Economics of the Software and Internet Industries, Toulouse, France. Online: `http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf` [22.02.2007].

Anderson, R. J. and T. Moore (2007b). Information Security Economics – And Beyond. In: A. Menezes (Ed.), *Advances in Cryptology – CRYPTO 2007*, Volume 4622 of *Lecture Notes in Computer Science*, Heidelberg, pp. 68–91. Springer.

Anderson, R. J., T. Moore, S. Nagaraja, and A. Ozment (2007). Incentives and Information Security. In: T. Roughgarden, E. Tardos, and V. V. Vazirani (Eds.), *Algorithmic Game Theory*. New York: Cambridge University Press.

Au, L., S. Nan, and P. Zhang (2007). Women Migrant Workers under the Chinese Social Apartheid. Committee for Asian Women (CAW).

Aubert, B. A., S. Dussault, M. Patry, and S. Rivard (1999). Managing the Risk of IT Outsourcing. In: *Proceedings of the 32nd Annual Hawaii International Conference on System Sciences*. DOI: 10.1109/HICSS.1999.772972.

Aubert, B. A., M. Patry, and S. Rivard (1998). Assessing the Risk of IT Outsourcing. In: *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, Volume 6, pp. 685–692.

Axelrod, C. W. (2004). *Outsourcing Information Security*. Norwood: Artech House.

Baskerville, R. F. (2003). Hofstede never studied culture. *Accounting, Organizations and Society 28*(1), 1–14.

Bedford, O. A. (2004). The Individual Experience of Guilt and Shame in Chinese Culture. *Culture & Psychology 10*(1), 29–52.

Bedford, O. A. and K.-K. Hwang (2003). Guilt and Shame in Chinese Culture: A Cross-cultural Framework from the Perspective of Morality and Identity. *Journal for the Theory of Social Behaviour 33*(2), 127–144.

Benedict, R. (1989). *Patterns of Culture*. Boston: Houghton Mifflin.

Benedict, R. (2005). *The Chrysanthemum and the Sword: Patterns of Japanese Culture*. New York: Houghton Mifflin.

Berry, J. W., Y. H. Poortinga, M. H. Segall, and P. R. Dasen (2002). *Cross-Cultural Psychology. Research and Applications* (Second ed.). Cambridge: Cambridge University Press.

BITS (2003). *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* (Second ed.).. Online: `http://www.bits.org/downloads/Publications%20Page/bits2003framework.pdf` [23.05.2007].

Björck, F. (2001). Security Scandinavian Style. Online: `http://www.dsv.su.se/~bjorck/files/bjorck-thesis.pdf` [12.12.2006].

Boeing (1996). Statistical Summary of Commercial Jet Aircraft Accidents. Worldwide operations. 1959-1995.

Boeing (2008). Statistical Summary of Commercial Jet Aircraft Accidents. Worldwide operations. 1959-2007. Online: `http://www.boeing.com/news/techissues/pdf/statsum.pdf` [19.01.2009].

Bond, M. H. (1991). *Beyond the Chinese Face: Insights from Psychology*. Hong Kong: Oxford University Press.

Bonin, J. P. and Y. Huang (2001). Dealing with the Bad Loans of the Chinese Banks. *Journal of Asian Economics 12*(2), 197–214.

Booth, W. C., G. G. Colomb, and J. M. Williams (2003). *The Craft of Research* (Second ed.). Chicago: The University of Chicago Press.

Boston Consulting Group (2005). IT Outsourcing and Offshoring: Hype or Opportunity? IT Cost Benchmarking in the European Banking Industry. Online: `http://www.bcg.com/impact_expertise/publications/files/IT_Outsourcing_Offshoring_Hype_Opportunity_IT_Benchmarking_European_Banks_Jun2005.pdf` [12.04.2008].

Bosworth, S. and M. E. Kabay (Eds.) (2002). *Computer Security Handbook* (Fourth ed.). New York: Wiley.

Brahm, L. J. (Ed.) (2002). *China After WTO*. China Intercontinental Press.

Brahm, L. J. (2004). *Doing Business in China. The Sun Tzu Way*. Boston: Tuttle.

Brown, D. and S. Wilson (2005). *The Black Book of Outsourcing: How to Manage the Changes, Challenges, and Opportunities*. Hoboken: Wiley.

Brynjolfsson, E. J., T. W. Malone, V. Gurbaxani, and A. Kambil (1994). Does Information Technology Lead to Smaller Firms? *Management Science 40*(12), 1628–1644.

BSI (2005). *IT Baseline Protection Manual*. Federal Office for Information Security (BSI). Online: `http://www.bsi.de/english/gshb/manual/download/pdfversion.zip` [24.09.2006].

Carmel, E. and P. Tjia (2006). *Offshoring Information Technology: Sourcing and Outsourcing to a Global Workforce.* Cambridge: Cambridge University Press.

Carroll, L. (2000). *Alice's Adventures in Wonderland & Through the Looking-Glass.* London: Penguin Books.

Chan, T. S. (1999). *Consumer Behavior in Asia. Issues and Marketing Practice.* Binghamton: International Business Press.

Chang, G. and Q. Shao (2004). How much is the Chinese currency undervalued? A quantitative estimation. *China Economic Review 15*(3), 366–371.

Charmaz, K. (2005). Grounded Theory in the 21st Century: Applications for Advancing Social Justice Studies. In: N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research*, pp. 507–535. Thousand Oaks: Sage Publications.

Chase, M. S. and J. C. Mulvenon (2002). *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies.* Santa Monica: RAND (National Security Research Division).

Chase, S. E. (2005). Narrative Inquiry. Multiple Lenses, Approaches, Voices. In: N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research*, pp. 651–679. Thousand Oaks: Sage Publications.

Chen, J. (1999). *Chinese Law: Towards an Understanding of Chinese Law, Its Nature, and Development.* The London-Leiden Series on Law, Administration and Development. The Hague: Kluwer Law International.

Chen, J. and B. M. Fleisher (1996). Regional Income Inequality and Economic Growth in China. *Journal of Comparative Economics 22*(2), 141–164.

Chhokar, J. S., F. C. Brodbeck, and R. J. House (Eds.) (2008). *Culture and Leadership Across the World. The GLOBE Book of In-Depth Studies of 25 Societies.* New York: Lawrence Erlbaum Associates.

Chinese Culture Connection (1987). Chinese values and the search for culture-free dimensions of culture. *Journal of Cross-Cultural Psychology 18*(2), 143–164.

Cialdini, R. B. (2001). *Influence: Science and Practice.* Needham Heights: Allyn & Bacon.

Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion.* New York: Harper Collins.

Clarke, D., P. Murrell, and S. Whiting (2005). Law, Institutions, and Property Rights in China. *Woodrow Wilson International Center for Scholars. Asia Program Special Report* (129).

Clarke, D., P. Murrell, and S. Whiting (2007). The Role of Law in China's Economic Development. *The George Washington University Law School. Public Law and Legal Theory Working Paper* (187).

Clarke, D. C. (1996). Power and Politics in the Chinese Court System: The Enforcement of Civil Judgements. *Columbia Journal of Asian Law 10*(1).

Clarke, D. C. (2002). Empirical Research into the Chinese Judicial System.

Clarke, D. C. (2003a). China's Legal System and the WTO: Prospects for Compliance. *Washington University Global Studies Law Review 2*(97), 97–120.

Clarke, D. C. (2003b). Empirical Research in Chinese Law. In: E. Jensen and T. Heller (Eds.), *Beyond Common Knowledge: Empirical Approaches to the Rule of Law*, pp. 164–192. Stanford: Stanford University Press.

Clayton, J. (1911). *The Rise of the Democracy.* London: Cassell and Company.

Clayton, R., S. J. Murdoch, and R. N. M. Watson (2006). Ignoring the Great Firewall of China. In: G. Danezis and P. Golle (Eds.), *Privacy Enhancing Technologies*, Volume 4258 of *Lecture Notes in Computer Science*, Heidelberg, pp. 20–35. Springer.

Clegg, S., M. Kornberger, and T. Pitsis (2005). *Managing and Organizations: An Introduction to Theory and Practice.* London: Sage Publications.

CMMI Product Team (2006). *CMMI for Development, Version 1.2: Improving processes for better products.* Pittsburgh: Carnegie Mellon Software Engineering Institute.

CNNIC (2006). Internet Connection Map of China. China Internet Network Information Center. Online: `http://www.cnnic.net.cn/images/info-stat/map0612.jpg` [12.09.2007].

Committee on Governmental Affairs (2000). *Cyber attack: Is the government safe? Hearing before the Committee on Governmental Affairs, United States Senate, One Hundred Sixth Congress.* Washington, D.C.: U.S. Government Printing Office. Online: `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_senate_hearings&docid=f:63639.pdf` [21.01.2009].

Committee on National Security Systems (2006). *National Information Assurance (IA) Glossary.* Fort Meade: National Security Agency. Online: `http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf` [23.08.2007].

Condon, J. C. and F. S. Yousef (1985). *An Introduction to Intercultural Communication.* New York: Macmillan Publishing Company.

Congressional-Executive Commision on China (2005). Senior Chinese Officials Acknowledge Rising Social Unrest, But Rule Out Political Liberalization. Human Rights and Rule of Law. Online: `http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=17209` [21.07.2008].

Craig, E. (Ed.) (1998). *Routledge Encyclopedia of Philosophy*, Volume 5. London: Routledge.

Dainton, M. and E. D. Zelley (2004). *Applying Communication Theory for Professional Life: A Practical Introduction.* Thousand Oaks: Sage Publications.

Dan Goodley, Rebecca Lawthom, P. C. and M. Moore (2004). *Researching Life Stories: Method, Theory and Analyses in a Biographical Age.* London: RoutledgeFalmer.

Day, D. V., S. J. Zaccaro, and S. M. Halpin (2004). *Leader Development for Transforming Organizations: Growing Leaders for Tomorrow.* Mahwah: Lawrence Erlbaum Associates.

DeLacey, B. J., K. Herman, D. J. Kiron, J. Lerner, and W.-S. Lo (2006). Government Intervention in Standardization: The Case of WAPI. Online: `http://ssrn.com/abstract=930930` [19.7.2008].

Deloitte (2005). *2005 Global Security Survey.* Online: `http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritySurvey_2005-07-21.pdf` [21.08.2008].

Deloitte (2006). *2006 Global Security Survey.* Online: `http://www.deloitte.com/dtt/cda/doc/content/us_fsi_150606globalsecuritysurvey(1).pdf` [21.08.2008].

Deloitte (2007). *2007 Global Security Survey.* Online: `http://www.deloitte.com/dtt/cda/doc/content/ca_en_Global_Security_Survey.final.en.pdf` [21.08.2008].

Denzin, N. K. and Y. S. Lincoln (2005a). The Discipline and Practice of Qualitative Research. In: N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research*, pp. 1–32. Thousand Oaks: Sage Publications.

Denzin, N. K. and Y. S. Lincoln (2005b). Methods of Collecting and Analyzing Empirical Materials. In: N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research*, pp. 641–649. Thousand Oaks: Sage Publications.

Dhillon, G. S. (1995). *Interpreting the Management of Information Systems Security.* Ph. D. thesis, University of London.

Dietl, H. (1993). *Institutionen und Zeit.* Tübingen: Mohr Siebeck.

Dilthey, W. (1972). The Rise of Hermeneutics. *New Literary History 3*(2), 229–244.

Dong, Q. and Y.-F. L. Lee (2007). The Chinese Concept of Face: A Perspective for Business Communicators. *Southwest Decision Sciences Institute.* Online: `http://www.swdsi.org/swdsi07/2007_proceedings/papers/401.pdf` [05.06.2008].

Dubin, R. (1960). Parsons' Actor: Continuities in Social Theory. *American Sociological Review 25*(4), 457–466.

Dutcher, J. W., K. Carrick, and S. M. Smith (2002). Flight Safety Attitudes and Human Factors Training. *5th International Workshop on Human Error, Safety, and Systems Development.*

Dyer, J. (1997). How Chrysler Created an American Keiretsu. *The Journal of Product Innovation Management 14*(2), 128–129.

Eagles, M., L. Johnston, L. W. Johnston, and C. Holoman (2003). *Politics: An Introduction to Democratic Government.* Peterborough: Broadview Press.

Earley, P. C. (1997). *Face, Harmony, and Social Structure: An Analysis of Organizational Behavior Across Cultures.* New York: Oxford University Press.

Edelman, B. (2003). Web Sites Sharing IP Addresses: Prevalence and Significance. Online: `http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/` [25.07.2008].

Edmonds, R. L. (Ed.) (2002). *China and Europe since 1978: A European Perspective.* Number 2 in The China Quarterly Special Issues. Cambridge: Cambridge University Press.

Electronic Data Systems (2007). Timeline: History Of EDS From Perot to IT Now. Online: `http://www.eds.com/about/history/timeline.aspx` [21.09.2008].

Ellickson, R. C. (1991). *Order Without Law: How Neighbors Settle Disputes.* Cambridge: Harvard University Press.

Eltschinger, C. (2007). *Source Code China. The New Global Hub of IT Outsourcing.* Hoboken: Wiley.

Facey, G. (2008). Risk Management in China: Outsourcing and Investment. In: J. Reuvid (Ed.), *Business Insights: China. Practical Advice on Entry Strategy and Engagement*, pp. 65–76. Kogan Page.

Fallows, J. (2008). The Connection Has Been Reset. The Atlantic. Online: `http://www.theatlantic.com/doc/200803/chinese-firewall` [16.07.2008].

Federal Communications Commission (1996). *Telecommunications Act of 1996* (Pub. LA. No. 104-104, 110 Stat. 56 ed.).

Flick, U. (2006). *An Introduction to Qualitative Research.* London: Sage Publications.

Fontana, A. and J. H. Frey (2005). The Interview. From Neutral Stance to Political Involvement. In: N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research*, pp. 695–727. Thousand Oaks: Sage Publications.

Friedman, T. L. (2000). *The Lexus and the Olive Tree.* New York: Anchor Books.

Friedman, T. L. (2005). *The World Is Flat.* London: Penguin Books.

Friedman, T. L. (2006). Bring in the Green Cat. Online: `http://select.nytimes.com/2006/11/15/opinion/15friedman.html` [21.08.2008].

Furubotn, E. G. and R. Richter (2005). *Institutions and Economic Theory: The Contribution of the New Institutional Economics.* University of Michigan Press.

Gadamer, H.-G. (2004). *Truth and Method. Question What You Thought Before* (Second ed.). London: Continuum.

Gallagher, T. (2001). The Value Orientations Method: A Tool to Help Understand Cultural Differences. *Journal of Extension 39*(6).

Glaser, B. (2002a). Constructivist Grounded Theory. *Forum: Qualitative Social Research 3*(3).

Glaser, B. (2004). Naturalist Inquiry and Grounded Theory. *Forum: Qualitative Social Research 5*(1).

Glaser, B. G. (1978). *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory.* Mill Valley: Sociology Press.

Glaser, B. G. (1998). *Doing Grounded Theory: Issues and Discussions.* Mill Valley: Sociology Press.

Glaser, B. G. (2001). *The Grounded Theory Perspective: Conceptualisation Contrasted with Description.* Mill Valley: Sociology Press.

Glaser, B. G. (2002b). Conceptualization: On Theory and Theorizing Using Grounded Theory. *International Journal of Qualitative Methods 1*(2), 1–31.

Glaser, B. G. and A. L. Strauss (1965). *Awareness of Dying.* Chicago: Aldine.

Glaser, B. G. and A. L. Strauss (2006). *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Piscataway: AldineTransaction.

Glaser, T. (2005). Trends in der IT-Sicherheit aus Sicht der Praxis. Master's thesis, Technische Universität Berlin.

Glaser, T. and F. Pallas (2007). Information Security and Knowledge Management: Solutions Through Analogies? *SSRN eLibrary*. Online: `http://ssrn.com/paper=1014302` [23.08.2007].

Glaser, T. and F. Pallas (2008). Aktuelle Sicherheitsparadigmen und ökonomische Konflikte. In: P. Horster (Ed.), *D.A.CH. Security 2008. Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven.* syssec.

Goodrich, P. (1998). Legal Hermeneutics. In: E. Craig (Ed.), *Routledge Encyclopedia of Philosophy*, Volume 5. London: Routledge.

Graham, J. and N. Lam (2003). The Chinese Negotiation. *Harvard Business Review 81*(10), 82–91.

Guba, E. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Technology Research and Development 29*(2), 75–91.

Guba, E. G. and Y. S. Lincoln (1994). Competing Paradigms in Qualitative Research. In: *Handbook of Qualitative Research*, Volume 2, pp. 105–117. Thousand Oaks: Sage Publications.

Guba, E. G. and Y. S. Lincoln (2005). Paradigmatic Controversies, Contradictions, and Emerging Confluences. In: N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research*, pp. 191–215. Thousand Oaks: Sage Publications.

Halbwachs, M. and L. A. Coser (1992). *On Collective Memory.* Heritage of Sociology Series. Chicago: University Of Chicago Press.

Hall, E. T. (1960). The Silent Language of Overseas Business. *Harvard Business Review 38*(3), 87–96.

Hall, E. T. (1974). *Handbook for Proxemic Research.* Washington, D.C.: Society for the Anthropology of Visual Communication.

Hall, E. T. (1989a). *Beyond Culture.* New York: Anchor Books,U.S.

Hall, E. T. (1989b). *The Dance of Life.* New York: Anchor Books.

Hall, E. T. (1990a). *The Hidden Dimension.* New York: Anchor Books.

Hall, E. T. (1990b). *The Silent Language.* New York: Anchor Books.

Hall, E. T. (1994). Context and Meaning. In: L. A. Samovar and R. E. Porter (Eds.), *Intercultural Communication: A Reader* (Seventh ed.)., pp. 60–69. Belmont: Thomson Wadsworth.

Hall, E. T. (1995). *West of the Thirties: Discoveries Among the Navajo and Hopi.* New York: Anchor Books.

Hall, E. T. and M. R. Hall (1990a). *Hidden Differences. Doing Business with the Japanese.* New York: Anchor Books.

Hall, E. T. and M. R. Hall (1990b). *Understanding Cultural Differences: Germans, French, and Americans.* Yarmouth: Intercultural Press.

Hall, R. and C. Jones (1999). Why Do Some Countries Produce So Much More Output Per Worker Than Others? *The Quarterly Journal of Economics 114*(1), 83–116.

Hall, S. (1992). Encoding/decoding. In: S. Hall, D. Hobson, A. Lowe, and P. Willis (Eds.), *Culture, Media, Language*, pp. 128–138. London: Routledge.

Hampden-Turner, C. and F. Trompenaars (1993). *The Seven Cultures of Capitalism: Value Systems for Creating Wealth in the United States, Japan, Germany, France, Britain, Sweden, and the Netherlands.* New York: Doubleday.

Hampden-Turner, C. and F. Trompenaars (2001). *Mastering the Infinite Game: How East Asian Values are Transforming Business Practices.* Oxford: Capstone.

Hampden-Turner, C., F. Trompenaars, and D. Lewis (2000). *Building Cross-Cultural Competence: How to Create Wealth from Conflicting Values.* New Haven: Yale University Press.

Hart, R. L. (2000). *Unfinished Man and the Imagination: Toward an Ontology and a Rhetoric of Revelation.* Louisville: Westminster John Knox Press.

Harvey, A. and J. Durbin (1986). The Effects of Seat Belt Legislation on British Road Casualties: A Case Study in Structural Time Series Modelling. *Journal of the Royal Statistical Society 149*(3), 187–227.

Hawking, S. W. (1998). *A Brief History of Time.* Toronto: Bantam Books.

He, H. Y. (2001). *Dictionary of the Political Thought of the People's Republic of China.* Armonk: M. E. Sharpe.

Helmreich, R. L. and A. C. Merritt (1998). *Culture at Work in Aviation and Medicine: National, Organizational, and Professional Influences.* Aldershot: Ashgate.

Helokunnas, T. and R. Kuusisto (2003). Information Security Culture in a Value Net. Engineering Management Conference 2003 (IEMC '03). Online: `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1252258&isnumber=28027` [25.03.2008].

Henderson, K. (2007). The Rule of Law and Judicial Corruption in China: Half-way Over the Great Wall. In: Transparency International (Ed.), *Global Corruption Report 2007. Corruption in Judicial Systems*, pp. 151–159. Cambridge: Cambridge University Press.

Hirschheim, R., A. Heinzl, and J. Dibbern (Eds.) (2006). *Information Systems Outsourcing: Enduring Themes, New Perspectives and Global Changes* (Second ed.). Berlin: Springer.

Ho, D. Y. (1976). On the Concept of Face. *American Journal of Sociology 81*(4), 867–884.

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

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations* (Second ed.). Thousand Oaks: Sage Publications.

Hofstede, G. (2003). *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations* (Second ed.). Thousand Oaks: Sage Publications.

Hofstede, G. and G. J. Hofstede (2005). *Cultures and Organizations: Software of the Mind* (second ed.). New York: Mcgraw-Hill.

Hollnagel, E. and D. D. Woods (2005). *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering.* Boca Raton: CRC Press.

Holstein, J. A. and J. F. Gubrium (2001). *Handbook of Interview Research: Context & Method.* Thousand Oaks: Sage Publications.

Holstein, J. A. and J. F. Gubrium (2003). *Inside Interviewing: New Lenses, New Concerns.* Thousand Oaks: Sage Publications.

House, R. J., P. J. Hanges, M. Javidan, P. W. Dorfman, and V. Gupta (Eds.) (2004). *Culture, Leadership, and Organizations. The GLOBE Study of 62 Societies.* Thousand Oaks: Sage Publications.

House, R. J., M. Javidan, P. J. Hanges, and P. W. Dorfman (2002). Understanding Cultures and Implicit Leadership Theories Across the Globe: An Introduction to Project GLOBE. *Journal of World Business 37*, 3–10.

Hughes, C. R. and G. Wacker (Eds.) (2003). *China and the Internet: Politics of the Digital Leap Forward.* London: Routledge.

Imai, M. (1986). *Kaizen (Ky'zen), the key to Japan's competitive success.* New York: McGraw-Hill.

Inglehart, R. (1971). The Silent Revolution in Europe: Intergenerational Change in Post-Industrial Societies. *American Political Science Review 65*(4), 991–1017.

Inglehart, R. (1977). *The Silent Revolution: Changing Values and Political Styles Among Western Publics.* Princeton: Princeton University Press.

Inglehart, R. (1990). *Culture Shift in Advanced Industrial Society.* Princeton: Princeton University Press.

Inglehart, R. (1997). *Modernization and Postmodernization: Cultural, Economic, and Political Change in 43 Societies.* Princeton: Princeton University Press.

Inglehart, R. (2004). *Human Beliefs and Values: A Cross-cultural Sourcebook Based on the 1999-2002 Values Surveys.* Mexico City: Siglo Veintiuno Editores.

Inglehart, R. and W. E. Baker (2000). Modernization, Cultural Change, and the Persistence of Traditional Values. *American Sociological Review 65*(1), 19–51.

Inkeles, A. and D. Levinson (1969). National Character: The Study of Modal Personality and Sociocultural Systems. In: G. Lindzey and E. Aronson (Eds.), *The Handbook of Social Psychology*, Volume 4, pp. 418–506. New York: McGraw-Hill.

Inkeles, A. and D. J. Levinson (1997). *National Character: A Psycho-Social Perspective.* New Brunswick: Transaction Publishers.

Ip, C., S. Hodges, and D. Ho (2003). Tackling the Challenges of Moving IT Activities Offshore. *McKinsey on IT 3*, 103–117.

ISO / IEC (2005a). ISO / IEC 17799:2005(E) – Information Technology – Security Techniques – Code of Practice for Information Security Management. International Organization for Standardization and International Electrotechnical Commission.

ISO / IEC (2005b). ISO / IEC 27001:2005(E) – Information Technology – Security Techniques – Information Security Management Systems – Requirements. International Organization for Standardization and International Electrotechnical Commission.

IT Governance Institute (2007). Cobit 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models. Online: `http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/MembersOnly.cfm&ContentFileID=14002` [25.05.2007].

Iyengar, P. (2008). *'India-3' are the Emerging Megavendors.* Gartner. Online: `http://www.gartner.com/DisplayDocument?id=713207` [17.01.2009].

Jacobs, J. B. (1976). A Preliminary Model of Particularistic Ties in Chinese Political Alliances: Kan-ch'ing and Kuan-hsi in a Rural Taiwanese Township. *The China Quarterly 78*, 237–273.

Jacobs, J. B. (1991). Elections in China. *The Australian Journal of Chinese Affairs* (25), 171–199.

Janssen, W. (1994). Seat-belt wearing and driving behavior: An instrumented-vehicle study. *Accident Analysis and Prevention 26*(2), 249–61.

Jick, T. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly 24*(4), 602–611.

Jing, H.-S. (2004). Differentiated order in the cockpit. *Human Factors and Aerospace Safety 4*(2), 131–143.

Kalish, I. (2004). China at a Crossroads. Seven Risks of Doing Business. Online: `http://www.deloitte.com/dtt/cda/doc/content/DTT_DR_ChinaCrossRd_Sept2004a.pdf` [21.08.2007].

Kampf, C. (1999). Building a theoretical framework for intercultural communication in technical communication pedagogy. *Professional Communication Conference 1999 (IPCC 99). Communication Jazz: Improvising the New International Communication Culture*, 151–158. DOI: 10.1109/IPCC.1999.799115.

Kaufmann, D., A. Kraay, and M. Mastruzzi (2007). The Worldwide Governance Indicators Project: Answering the Critics. World Bank Policy Research Working Paper 4149. Online: `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=965077` [15.05.2008].

Keene, D. (1959). *Living Japan.* Garden City: Doubleday.

Kennedy, G. and D. Clark (2006). Outsourcing to China – Risks and Benefits. *Computer Law & Security Report 22*, 250–253.

Kerckhoffs, A. (1883a). La Cryptographie Militaire. *Journal des Sciences Militaires IX*, 5–38.

Kerckhoffs, A. (1883b). La Cryptographie Militaire. *Journal des Sciences Militaires IX*, 161–191.

Kim, D., Y. Pan, and H. Park (1998). High-Versus Low-Context Culture: A Comparison of Chinese, Korean, and American Cultures. *Psychology and Marketing 15*(6), 507–521.

Kluckhohn, A. L. and C. Kroeber (1952). *Culture: A Critical Review of Concepts and Definitions*. Cambridge: Peabody Museum of Archaeology and Ethnology, Harvard University.

Kluckhohn, C. (1927). *To the Foot of the Rainbow*. New York: Century.

Kluckhohn, C. (1933). *Beyond the Rainbow*. Boston: The Christopher Publishing House.

Kluckhohn, C. (1944). *Navaho Witchcraft*. Boston: Beacon Press.

Kluckhohn, C. (1949). *Mirror for Man: The Relation of Anthropology to Modern Life*. New York: Whittlesey House.

Kluckhohn, C. (1951). Values and Value-Orientation in the Theory of Action. In: T. Parsons and E. A. Shils (Eds.), *Toward a General Theory of Action*, pp. 388–433. Cambridge: Harvard University Press.

Kluckhohn, C. and H. A. Murray (Eds.) (1948). *Personality: In Nature, Society and Culture*. New York: Knopf.

Kluckhohn, C. and L. C. Wyman (1940). *An Introduction to Navaho Chant Practice*. Menasha: American Anthropological Association.

Kluckhohn, F. R. and F. L. Strodtbeck (1961). *Variations in Values Orientations*. Evanston: Row Paterson.

Kohls, L. R. and J. M. Knight (1994). *Developing Intercultural Awareness: A Cross-cultural Training Handbook*. Yarmouth: Intercultural Press.

Koops, B.-J. (2008). Crypto Law Survey. Online: `http://rechten.uvt.nl/koops/cryptolaw/cls2.htm` [19.7.2008].

Kromrey, H. (2005). Qualitativ vs. Quantitativ – Ideologie oder Realität? 1. Berliner Methodentreffen Qualitative Forschung. Online: `http://www.berliner-methodentreffen.de/material/2005/kromrey.pdf` [07.03.2007].

Kutschker, M. and S. Schmid (2006). *Internationales Management*. München: Oldenbourg Wissenschaftsverlag.

Kuusisto, R., K. Nyberg, and T. Virtanen (2004). Unite Security Culture. *Proceedings of 3rd European Conference on Information Warfare and Security, Royal Holloway University of London*, 221–229.

Lacity, M. C. and R. Hirschheim (1993). *Information Systems Outsourcing: Myths, Metaphors and Realities*. Chichester: Wiley.

Lacity, M. C. and L. P. Willcocks (2001). *Global Information Technology Outsourcing: In Search of Business Advantage*. Chichester: Wiley.

Le Goff, J. (1992). *History and Memory*. New York: Columbia University Press.

Lessig, L. (1998a). The Architecture of Privacy. Taiwan Net '98. Online: `http://www.lessig.org/content/articles/works/architecture_priv.pdf` [17.01.2007].

Lessig, L. (1998b). The New Chicago School. *The Journal of Legal Studies 27*(2), 661–691. Online: `http://www.lessig.org/content/articles/works/LessigNewchicschool.pdf` [10.01.2007].

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books.

Lever, S. (1997). An Analysis of Managerial Motivations Behind Outsourcing Practices in Human Resources. *Human Resource Planning 20*(2).

Levine, D. E. (2002). Using Encryption Internationally. In: S. Bosworth and M. E. Kabay (Eds.), *Computer Security Handbook* (Fourth ed.)., Chapter 50. New York: Wiley.

Lewis, R. D. (2005). *When Cultures Collide: Leading Across Cultures* (Third ed.). Boston: Nicholas Brealey.

Li, L. (2003). The Empowering Effect of Village Elections in China. *Asian Survey 43*(4), 648–662.

Li, W.-C. and D. Harris (2007). Confucius in Western Cockpits: The Investigation of Long-Term Versus Short-Term Orientation Culture and Aviation Accidents. In: D. Harris (Ed.), *Engineering Psychology and Cognitive Ergonomics*, Volume 4262 of *Lecture Notes in Computer Science*, Heidelberg, pp. 716–722. Springer.

Lieberthal, K. and G. Lieberthal (2004). The Great Transition. In: *Harvard Business Review on Doing Business in China*, pp. 1–30. Boston: Harvard Business School Press.

Lin-Liu, J. (2004). Top U.S. Officials Successfully Defend IEEE's Wi-Fi Standard. *IEEE Spectrum 41*(6), 16–17.

Lincoln, Y. and E. Guba (1985). *Naturalistic Inquiry*. Newbury Park: Sage Publications.

Littlejohn, S. W. (2003). *Theories of Human Communication*. Beijing: Tsinghua University Press.

Liu, H. and L. Roos (2006). Managing strategic planning paradigms in China. *Marketing Intelligence & Planning 24*(5), 432–445.

Locke, K. (2001). *Grounded Theory in Management Research*. London: Sage Publications.

Ma, G. and B. S. C. Fung (2002). China's Asset Management Corporations. *Bank for International Settlements. Monetary and Economic Department. BIS Working Papers* (115).

Mallery, J., R. Hurwitz, and G. Duffy (1986). Hermeneutics: From Textual Explication to Computer Understanding? *Massachusetts Institute of Technology, Artificial Intelligence Laboratory, AI Memo No. 871*. Online: `http://hdl.handle.net/1721.1/6438` [13.11.2008].

Malone, T. W. (2004). *The Future of Work: How the New Order of Business Will Shape Your Organization, Your Management Style, and Your Life.* Boston: Harvard Business School Press.

Malone, T. W., J. Yates, and R. I. Benjamin (1987). Electronic Markets and Electronic Hierarchies. *Communications of the ACM 30*(6), 484–497.

Mankiw, N. G. and M. P. Taylor (2006). *Economics.* London: Thomson Learning.

Marschan-Piekkari, R. and C. Welch (2004). *Handbook of Qualitative Research Methods for International Business.* Cheltenham: Edward Elgar Publishing.

Marshall, D., R. Lamming, B. Fynes, and S. de Búrca (2005). The Development of an Outsourcing Process Model. *International Journal of Logistics 8*(4), 347–359.

Maslow, A. H. (1943). A Theory of Human Motivation. *Psychological Review 50*, 370–396.

Maslow, A. H. (1993). *The Farther Reaches of Human Nature.* New York: Arkana.

Maslow, A. H. (1998). *Toward a Psychology of Being.* New York: Wiley.

Mason, T. (1990). *Perot: An Unauthorized Biography.* New York: McGraw-Hill.

Mathison, S. (1988). Why Triangulate? *Educational Researcher 17*(2), 13–17.

McCarthy, J. C. and M. Hudson (2005). China's Realistic Offshore Role. Online: `http://www.forrester.com/go?docid=37409` [04.12.2007].

McCarthy, J. C., C. F. Ross, F. Bartolomey, and A. Thresher (2007). China's Diminishing Offshore Role. Online: `http://www.forrester.com/go?docid=42097` [04.12.2007].

McClelland, D. C. (1961). *The Achieving Society.* Princeton: D. Van Nostrand.

Merritt, A. C. (1998). Replicating Hofstede: A Study of Pilots in Eighteen Countries. In: R. Jensen (Ed.), *Proceedings of the Ninth International Symposium on Aviation Psychology*, pp. 667–672.

Merritt, A. C. (2000). Culture in the Cockpit: Do Hofstede's Dimensions Replicate? *Journal of Cross-Cultural Psychology 31*(3), 283–301.

Merritt, A. C. and R. L. Helmreich (1996). Human Factors on the Flight Deck: The Influence of National Culture. *Journal of Cross-Cultural Psychology 27*(1), 5–24.

Ministry of Commerce, People's Republic of China (2006). *Circular of Ministry of Commerce on Implementing the "Thousand-Hundred-Ten Project" of Service Outsourcing.* Online: `http://chinasourcing.mofcom.gov.cn/content2.jsp?id=19654` [23.06.2007].

Ministry of Information Industry, People's Republic of China (2000). *Telecommunications Regulations of People's Republic of China.* Online: `http://tradeinservices.mofcom.gov.cn/en/b/2000-09-25/18619.shtml` [23.06.2007].

Mitchell, C. (2000). *A Short Course in International Business Culture.* Novato: World Trade Press.

Mitnick, K. D. and W. L. Simon (2002). *The Art of Deception: Controlling the Human Element of Security.* Indianapolis: Wiley.

Miyashita, K. and D. W. Russell (1995). *Keiretsu: Inside the Hidden Japanese Conglomerates.* New York: McGraw-Hill.

Mjøs, K. (2004). Basic Cultural Elements Affecting the Team Function on the Flight Deck. *International Journal of Aviation Psychology 14*(2), 151–169.

Moores, T. (2003). The Effect of National Culture and Economic Wealth on Global Software Piracy Rates. *Communications of the ACM 46*(9), 207–215.

Neusner, J. (2004). *Neusner on Judaism.* Adlershot: Ashgate.

Neusner, J. and B. Chilton (1997). *The Intellectual Foundations of Christian and Jewish Discourse.* London: Taylor & Francis.

Newman, K. L. and S. D. Nollen (1996). Culture and Congruence: The Fit Between Management Practices and National Culture. *Journal of International Business Studies 27*(4), 753–779.

Norman, D. A. (1998). *The Design of Everyday Things.* New York: Basic Books.

North, D. C. (1990). *Institutions, Institutional Change and Economic Performance.* Cambridge: Cambridge University Press.

North, D. C. (2005). Institutions and the Performance of Economics Over Time. In: C. Ménard and M. M. Shirley (Eds.), *Handbook of New Institutional Economics*, pp. 21–30. Dordrecht: Springer.

Obeng, S. G. (1999). Apologies in Akan discourse. *Journal of Pragmatics 31*(5), 709–734.

O'Brien, K. J. (2001). Villagers, Elections, and Citizenship in Contemporary China. *Modern China 27*(4), 407–435.

O'Brien, K. J. (2008). Improving Election Procedures and Practices in China: Some Modest Proposals. Online: `http://ssrn.com/abstract=1157092` [20.07.2008].

O'Brien, K. J. and L. Li (2000). Accommodating "Democracy" in a One-Party State: Introducing Village Elections in China. *The China Quarterly* (162), 465–489.

OECD (2002). *Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security.* Online: `http://www.oecd.org/dataoecd/16/22/15582260.pdf` [13.05.2006].

OECD (2008). *Compendium of Patent Statistics.* Online: `http://www.oecd.org/dataoecd/5/19/37569377.pdf` [19.10.2008].

O'Neil, D. (2008). Modern Human Variation. An Introduction to An Introduction to Contemporary Human Biological Diversity. Online: `http://anthro.palomar.edu/vary/vary_2.htm` [16.06.2008].

OpenNet Initiative (2005). Internet Filtering in China in 2004-2005: A Country Study. Online: `http://ssrn.com/abstract=706681` [17.03.2008].

Orts, E. (2001). The Rule of Law in China. *Vanderbilt Journal of Transnational Law 34*(1), 43–115.

Ostrom, E. (2005). Doing Institutional Analysis. Digging Deeper Than Markets and Hierarchies. In: C. Ménard and M. M. Shirley (Eds.), *Handbook of New Institutional Economics*, pp. 819–848. Dordrecht: Springer.

Palmer, R. E. (1969). *Hermeneutics. Interpretation Theory in Schleiermacher, Dilthey, Heidegger, and Gadamer*. Evanston: Northwestern University Press.

Parker, B. (2005). *Introduction to Globalization and Business: Relationships and Responsibilities*. London: Sage Publications.

Parsons, T. (1949). *The Structure of Social Action: A Study in Social Theory with special reference to a group of Recent European Writers* (Second ed.). New York: Free Press.

Parsons, T. (1960). Pattern Variables Revisited: A Response to Robert Dubin. *American Sociological Review 25*(4), 467–483.

Parsons, T. (1991). *The Social System*. London: Routledge.

Parsons, T. and E. A. Shils (Eds.) (1951a). *Toward a General Theory of Action*. Cambridge: Harvard University Press.

Parsons, T. and E. A. Shils (1951b). Values, Motives, and Systems of Action. Systems of Value-Orientation. In: T. Parsons and E. A. Shils (Eds.), *Toward a General Theory of Action*. Cambridge: Harvard University Press.

Parsons, T. and E. A. Shils (Eds.) (2001). *Toward a General Theory of Action: Theoretical Foundations for the Social Sciences*. New Brunswick: Transaction Publishers.

Payr, S. and R. Trappl (2004). *Agent Culture: Human-agent Interaction in a Multicultural World*. London: Routledge.

Peerenboom, R. (2002). *China's Long March Toward Rule of Law*. Cambridge: Cambridge University Press.

Pei, M. (2007). Corruption Threatens China's Future. *Carnegie Endowment for International Peace. Policy Brief* (55).

Pickett, J. P. et al. (Eds.) (2000). *American Heritage Dictionary of the English Language* (Fourth ed.). Boston: Houghton Mifflin.

Picot, A., H. Dietl, and E. Franck (2005). *Organisation. Eine ökonomische Perspektive* (Fourth ed.). Stuttgart: Schäffer-Poeschel.

Picot, A., R. Reichwald, and R. Wigand (2008). *Information, Organization and Management*. Berlin: Springer.

Pierce, J. R. (1980). *An Introduction to Information Theory: Symbols, Signals and Noise*. New York: Dover.

Popkin, J. M. and P. Iyengar (2007). *IT And the East: How China And India Are Altering the Future of Technology And Innovation*. Boston: Harvard Business School Press.

Popper, K. R. (2002). *Conjectures and Refutations. The Growth of Scientific Knowledge*. London: Routledge.

Porter, R. E. and L. A. Samovar (1994). An Introduction to Intercultural Communication. In: R. E. Porter and L. A. Samovar (Eds.), *Intercultural Communication: A Reader* (Seventh ed.)., pp. 4–26. Belmont: Thomson Wadsworth.

Qu, Z. and M. Brocklehurst (2003). What will it take for China to become a competitive force in offshore outsourcing? An analysis of the role of transaction costs in supplier selection. *Journal of Information Technology 18*, 53–67.

Reporters Without Borders (2008). 2008 Annual Report. Freedom of the Press Worldwide in 2008. Online: `http://www.rsf.org/IMG/pdf/rapport_en-2.pdf` [23.11.2008].

Richardson, L. and E. A. S. Pierre (2005). Writing – A Method of Inquiry. In: N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research*. Thousand Oaks: Sage Publications.

Richens, J., J. Imrie, and A. Copas (2000). Condoms and seat belts: The parallels and the lessons. *The Lancet 355*(9201), 400–403.

Richerson, P. J. and R. Boyd (2006). *Not by Genes Alone: How Culture Transformed Human Evolution*. Chicago: University Of Chicago Press.

Rose, G., R. Evaristo, and D. Straub (2003). Culture and consumer responses to web download time: A four-continent study of mono and polychronism. *IEEE Transactions on Engineering Management 50*(1), 31–44.

Ruey, Y. (1967). The Five Social Dyads as a Means of Social Control with a Review of the Li in Confucianism. *Journal of Sociology 3*, 47–58.

Salinger, S., L. Plonka, and L. Prechelt (2008). A Coding Scheme Development Methodology Using Grounded Theory for Qualitative Analysis of Pair Programming. *Human Technology: An Interdisciplinary Journal on Humans in ICT Environments 4*, 9–25.

Samovar, L. A. and R. E. Porter (Eds.) (1994). *Intercultural Communication: A Reader* (Seventh ed.). Belmont: Thomson Wadsworth.

Sasaki, R., S. Qing, E. Okamoto, and H. Yoshiura (Eds.) (2005). *Security and Privacy in the Age of Ubiquitous Computing*. IFIP International Federation for Information Processing. New York: Springer.

Sautedé, E. (2002). Telecoms in China: Towards a Post-WTO Shock Therapy? *China Perspectives* (41).

Sayo, P., J. G. Chacko, and G. Pradhan (Eds.) (2004). *ICT Policies and e-Strategies in the Asia-Pacific. A Critical Assessment of the Way Forward*. New Delhi: UNDP. Asia Pacific Development Information Programme, Elsevier. Online: `http://www.apdip.net/projects/igov/ict4dsayo-ch8.pdf` [23.11.2008].

Schaub, M. E. (2007). *China: The Art of Law – Chronicling Deals, Disasters, Greed, Stupidity and Occasional Success in the New China*. Hong Kong: CCH.

Schein, E. H. (1999). *The Corporate Culture Survival Guide*. San Francisco: Jossey-Bass.

Schein, E. H. (2004). *Organizational Culture and Leadership* (Third ed.). San Francisco: Jossey-Bass.

Scheuch, E. K. (1995). Theoretical Implications of Comparative Survey in Research: Why the Wheel of Cross-Cultural Methodology Keeps on Being Reinvented. In: A. Inkeles and M. Sasaki (Eds.), *Comparing Nations and*

Cultures: Readings in a Cross-Disciplinary Perspective. Englewood Cliffs: Prentice Hall.

Schleiermacher, F. (1998). *Hermeneutics and Criticism: And Other Writings*. Cambridge: Cambridge University Press.

Schlienger, T. and S. Teufel (2002). Information Security Culture: The Socio-Cultural Dimension in Information Security Management. In: A. Ghonaimy, M. T. El-Hadidi, and H. K. Aslan (Eds.), *Security in the Information Society: Visions and Perspectives*, Volume 214 of *IFIP Conference Proceedings*, Norwell, pp. 191–202. Kluwer.

Schlienger, T. and S. Teufel (2003a). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. *14th International Workshop on Database and Expert Systems Applications*, 405–409. DOI: 10.1109/DEXA.2003.1232055.

Schlienger, T. and S. Teufel (2003b). Information Security Culture – From Analysis to Change. *South African Computer Journal 31*, 46–52.

Schlienger, T. and S. Teufel (2005). Tool supported Management of Information Security Culture. In: R. Sasaki, S. Qing, E. Okamoto, and H. Yoshiura (Eds.), *Security and Privacy in the Age of Ubiquitous Computing*, New York, pp. 65–77. Springer.

Schneier, B. (2004). *Secrets and Lies: Digital Security in a Networked World*. Indianapolis: Wiley.

Schneier, B. (2006). *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Berlin: Springer.

Schneier, B. (2007). Information Security and Externalities. *ENISA Quarterly 2*(4), 3–4.

Schneier, B. (2008). The Psychology of Security. Online: `http://www.schneier.com/essay-155.pdf` [12.07.2008].

Schulz von Thun, F. (1981). *Miteinander reden 1: Störungen und Klärungen*. Reinbek: Rowohlt.

Schulz von Thun, F. (1989). *Miteinander Reden 2: Stile, Werte und Persönlichkeitsentwicklung*. Reinbek: Rowohlt.

Schulz von Thun, F., J. Ruppel, and R. Stratmann (2000). *Miteinander Reden: Kommunikationspsycholgoie für Führungskräfte*. Reinbek: Rowohlt.

Schwartz, P. (1996). *The Art of the Long View: Planning for the Future in an Uncertain World*. New York: Doubleday.

Schwartz, S. (1994). Beyond Individualism/Collectivism: New Cultural Dimensions of Values. In: U. Kim, H. Triandis, C. Kagitcibasi, S.-C. Choi, and G. Yoon (Eds.), *Individualism and collectivism: Theory, method, and applications*, Volume 18, pp. 85–119. Thousand Oaks: Sage Publications.

Schwartz, S. H. (1992). Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries. *Advances in Experimental Social Psychology 25*, 1–65.

Schwartz, S. H. (1999). A Theory of Cultural Values and Some Implications for Work. *Applied Psychology 48*(1), 23–47.

Sechrest, L. (1992). Roots: Back to Our First Generations. *American Journal of Evaluation 13*(1), 1–7.

Shambaugh, D. L. (1995). *Deng Xiaoping: Portrait of a Chinese Statesman.* Oxford: Oxford University Press.

Shannon, C. E. (1948, July, October). A Mathematical Theory of Communication. *Bell System Technical Journal 27*, 379–423, 623–656.

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal 28*(4), 656–715.

Shannon, C. E. (2001). A Mathematical Theory of Communication. *ACM SIGMOBILE Mobile Computing and Communications Review 5*(1), 3–55.

Shea, W. M. and P. A. Huff (1995). *Knowledge and Belief in America: Enlightenment Traditions and Modern Religious Thought (Woodrow Wilson Center Series).* Cambridge: Cambridge University Press.

Sherman, P. J., R. L. Helmreich, and A. C. Merritt (1997). National Culture and Flight Deck Automation: Results of a Multination Survey. *International Journal of Aviation Psychology 7*(4), 311–329.

Shi, T. (1999). Village Committee Elections in China: Institutionalist Tactics for Democracy. *World Politics 51*(3), 385–412.

Shostack, A. and A. Stewart (2008). *The New School of Information Security.* Boston: Addison Wesley.

Slay, J., K. Darzanos, G. Quirchmayr, and A. Koronios (2003). Towards a Mature Understanding of "Culture" in Information Systems Security Research. The International Federation for Information Processing (IFIP) Conference, Athens, Greece. Online: `http://www.aueb.gr/ifip-isglob03/proceedings/55%20-%20Slay.pdf` [12.03.2008].

Slingerland, E. (2004). Conceptions of the Self in the Zhuangzi: Conceptual Metaphor Analysis and Comparative Thought. *Philosophy East & West 54*(3), 322–342.

Smith, A. (1776). *An Inquiry into the Nature And Causes of the Wealth of Nations.* Library of Economics and Liberty. Online: `http://www.econlib.org/library/Smith/smWN.html` [23.09.2008].

Smith, P., S. Dugan, and F. Trompenaars (1996). National Culture and the Values of Organizational Employees: A Dimensional Analysis Across 43 Nations. *Journal of Cross-Cultural Psychology 27*(2), 231–264.

Söbbing, T. (2006). *Handbuch des IT-Outsourcing. Recht, Strategien, Prozesse, IT, Steuern, samt Business Process Outsourcing* (Third ed.). Heidelberg: C.F. Müller Verlag.

Soeters, J. L. and P. C. Boer (2000). Culture and Flight Safety in Military Aviation. *The International Journal of Aviation Psychology 10*(2), 111–133.

SOX (2002). Sarbanes-Oxley Act of 2002 – Public Company Accounting Reform and Investor Protection Act of 2002. One Hundred Seventh Congress of the United States of America, H. R. 3763. Online: `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf` [07.07.2005].

Spence, A. M. (1973). Job Market Signaling. *Quarterly Journal of Economics 87*(3), 355–374.

Spence, A. M. (1974). *Market Signaling: Informational Transfer in Hiring and Related Screening Processes*. Cambridge: Harvard University Press.

Spence, J. D. (1991). *The Search for Modern China*. New York: Norton.

Spencer-Oatey, H. (2000). Introduction: Language, Culture and Rapport Management. In: H. Spencer-Oatey (Ed.), *Culturally Speaking: Managing Rapport in Talk Across Cultures*, pp. 1–8. London: Continuum.

Stake, R. E. (2005). Qualitative Case Studies. In: N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research*. Thousand Oaks: Sage Publications.

Stees, J. (1998). *Outsourcing Security: A Guide for Contracting Services*. Woburn: Butterworth-Heinemann.

Stewart, W. (2001). *Deng Xiaoping: Leader in a Changing China*. Minneapolis: Lerner.

Stiglitz, J. E. (1973). The Theory of Screening, Education, and the Distribution of Income. *Cowles Foundation for Research in Economics at Yale University* (354).

Stiglitz, J. E. (2000). Capital Market Liberalization, Economic Growth, and Instability. *World Development 28*(6), 1075–1086.

Stipek, D. (1998). Differences between Americans and Chinese in the Circumstances Evoking Pride, Shame, and Guilt. *Journal of Cross-Cultural Psychology 29*(5), 616–629.

Straub, D., K. Loch, R. Evaristo, E. Karahanna, and M. Srite (2002). Toward a theory-based measurement of culture. *Journal of Global Information Management 10*(1), 13–23.

Strauss, A. L. (1987). *Qualitative Analysis for Social Scientists*. Cambridge: Cambridge University Press.

Tanner, M. S. (2004). China Rethinks Unrest. *The Washington Quarterly 27*(3), 137–156.

Terwey, M. (2000). ALLBUS: A German General Social Survey. In: G. Wagner (Ed.), *Schmollers Jahrbuch*, Zeitschrift für Wirtschafts- und Sozialwissenschaften (Journal of Applied Social Science Studies). Berlin: Duncker & Humblot.

The Economist (2003). China – Eating your Lunch? *The Economist. February 15th, 2003*.

The Economist (2006). The Myth of Chindia. Online: `http://economist.com/daily/columns/asiaview/displaystory.cfm?story_id=8311987` [22.11.2006].

Thomas, D. C. (2001). *Essentials of International Management: A Cross-cultural Perspective*. Thousand Oaks: Sage Publications.

Transparency International (2008a). Annual Report 2007. Online: `http://www.transparency.org/content/download/33964/529096` [21.07.2008].

Transparency International (2008b). Global Corruption Report 2008. Corruption in the Water Sector. Online: `http://www.transparency.org/content/download/32994/505946` [21.07.2008].

Treviño, A. J. (2001). *Talcott Parsons Today: His Theory and Legacy in Contemporary Sociology*. Lanham: Rowman & Littlefield Publishers.

Triandis, H. C. (1995). *Individualism & Collectivism*. Boulder: Westview Press.

Trompenaars, F. and C. Hampden-Turner (1997). *Riding the Waves of Culture: Understanding Cultural Diversity in Business*. London: Nicholas Brealey.

Trompenaars, F. and C. Hampden-Turner (2004). *Managing People Across Cultures*. London: Capstone.

Tsui, A. S. and J.-L. L. Farh (1997). Where Guanxi Matters: Relational Demography and Guanxi in the Chinese Context. *Work and Occupations 24* (1), 56.

Turner, J. C. (1982). Towards a cognitive redefinition of the social group. In: H. Tajfel (Ed.), *Social identity and intergroup relations*, pp. 15–40. Cambridge: Cambridge University Press.

Tylor, E. B. (1871). *Primitive Culture: Researches into the Development of Mythology, Philosophy, Religion, Art and Custom*. London: John Murray.

Ulrich, P., J. G. Chacko, and P. Sayo (2004). Overview of ICT Policies and e-Strategies in the Asia-Pacific Region. In: P. Sayo, J. G. Chacko, and G. Pradhan (Eds.), *ICT Policies and e-Strategies in the Asia-Pacific. A Critical Assessment of the Way Forward*, pp. 1–55. New Delhi: UNDP. Asia Pacific Development Information Programme, Elsevier.

UNDP (2007). *Human Development Report 2007/2008*. New York: United Nations Development Programme. Online: `http://hdr.undp.org/en/media/HDR_20072008_EN_Complete.pdf` [06.06.2008].

UNESCO (2002). UNESCO Universal Declaration on Cultural Diversity. Online: `http://www.unesco.org/education/imld_2002/unversal_decla.shtml` [13.01.2007].

United Nations (2008). *The Millennium Development Goals Report 2008*. New York. Online: `http://www.un.org/millenniumgoals/pdf/The%20Millennium%20Development%20Goals%20Report%202008.pdf` [13.06.2008].

Ure, J. (2002). China's Telecommunications and IT: Planning and the WTO? *Working Paper. University of Hong Kong*. Online: `http://www.trp.hku.hk/papers/2002/china_planning_wto.pdf` [02.11.2006].

Van Maanen, J. (Ed.) (1983). *Qualitative Methodology*. Beverly Hills: Sage Publications.

Van Oorschot, M. and M. Hogerhuis (2006). *How People Get Lost in Organizations: On Communication and Organizing. An Anthropological Search*. Delft: Eburon Academic Publishers.

Vanhonacker, W. (2004). Entering China: An Unconventional Approach. In: *Harvard Business Review on Doing Business in China*, pp. 105–121. Boston: Harvard Business School Press.

Varian, H. (2004). System Reliability and Free Riding. Online: `http://www.sims.berkeley.edu/~hal/Papers/2004/reliability.pdf` [27.02.2007].

Victor, D. (1992). *International Business Communication*. New York: Harper Collins.

von Jouanne-Diedrich, H. (2004). 15 Jahre Outsourcing-Forschung: Systematisierung und Lessons Learned. In: R. Zarnekow, W. Brenner, and H. H. Grohmann (Eds.), *Informationsmanagement. Konzepte und Strategien für die Praxis*, pp. 125–133. Heidelberg: dpunkt Verlag.

von Solms, B. (2000). Information Security – The Third Wave? *Computers & Security 19*, 615–620. DOI: 10.1016/S0167-4048(00)07021-8.

von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security 25*, 165–168. DOI: 10.1016/j.cose.2006.03.004.

von Solms, B. and R. von Solms (2005). From information security to ... business security? *Computers & Security 24*(4), 271–273.

Wacker, G. (2003). The Internet and Censorship in China. In: C. R. Hughes and G. Wacker (Eds.), *China and the Internet: Politics of the Digital Leap Forward*. London: Routledge.

Wadhwa, V. and G. Gereffi (2005). Framing the Engineering Outsourcing Debate: Placing the United States on a Level Playing Field with China and India. Online: `http://ssrn.com/abstract=1015831` [23.03.2008].

Wagner, S. and L. Dittmar (2006). The unexpected benefits of Sarbanes-Oxley. *Harvard Business Review 84*(4), 133–140.

Walton, G. (2001). *China's Golden Shield. Corporations and the Development of Surveillance Technology in the People's Republic of China.* International Centre for Human Rights and Democratic Development. Online: `http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF` [29.01.2009].

Wang, Y. (2001). *Chinese Legal Reform: The Case of Foreign Investment Law*. East Asian Economics and Business Series. London: Routledge.

Watzlawick, P., J. B. Bavelas, and D. D. Jackson (1967). *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes*. New York: Norton.

Weiner, B. (1996). *Human Motivation: Metaphors, Theories, and Research*. Thousand Oaks: Sage Publications.

Werfelman, L. (2008). Language Barrier. *AeroSafety World*, 41–43. Online: `http://www.flightsafety.org/asw/aug08/asw_aug08.pdf` [18.09.2008].

Wernick, C. (2007). *Strategic Investment Decisions in Regulated Markets. The Relationship Between Infrastructure Investments and Regulation in European Broadband*. Wiesbaden: Deutscher Universitäts-Verlag.

West-Newman, C. L. (2006). Feeling for Justice? Rights, Laws, and Cultural Contexts. *Law & Social Inquiry 30*(2), 305–335.

Whaley, B. B. and W. Samter (Eds.) (2007). *Explaining Communication: Contemporary Theories and Exemplars.* Mahwah: Lawrence Erlbaum Associates.

Whitehouse, D. (2006). Chinese workers and peasants in three phases of accumulation. Delivered at the Colloquium on the Economy, Society and Nature 2006. Centre for Civil Society at the University of KwaZulu-Natal.

Whitman, M. E. and H. J. Mattord (2003). *Principles of Information Security.* Beijing: Tsinghua University Press.

Wiener, N. (1961). *Cybernetics. Or Control and Communication in the Animal and the Machine.* Cambridge: MIT Press.

Wiener, N. (1988). *The Human Use of Human Beings: Cybernetics and Society.* New York: Da Capo Press.

Williams, R. (1976). *Keywords: A Vocabulary of Culture and Society.* Oxford: Oxford University Press.

Winograd, T. and F. Flores (1986). *Understanding Computers and Cognition: A New Foundation for Design.* Norwood: Ablex.

Witzel, A. (1982). *Verfahren der qualitativen Sozialforschung. Überblick und Alternativen.* Frankfurt am Main: Campus Verlag.

Witzel, A. (1989). Das problemzentrierte Interview. In: *Qualitative Forschung in der Psychologie. Grundfragen, Verfahrensweisen, Anwendungsfelder*, pp. 227–256. Heidelberg: Asanger Roland Verlag.

Witzel, A. (1996). *Auswertung problemzentrierter Interviews. Grundlagen und Erfahrungen*, pp. 49–76. Baden Baden: Nomos.

Witzel, A. (2000). The problem-centered interview. *Forum: Qualitative Social Research 1*(1).

Wolfe, A. (2007). Taiwan Quake Exposes Internet Vulnerability. PINR. Power and Interest News Report. Online: `http://www.pinr.com/report.php?ac=view_report&report_id=602` [18.07.2008].

Wolfgarten, S. (2006). Investigating large-scale Internet content filtering. Online: `http://www.devtarget.org/downloads/dcu-mssf-2005-wolfgarten-filtering.pdf` [25.07.2008].

Womack, B. (1982). The 1980 County-Level Elections in China: Experiment in Democratic Modernization. *Asian Survey 22*(3), 261–277.

World Bank (2007). *World Development Indicators 2007.* Washington, D.C.: International Bank for Reconstruction and Development, The World Bank.

Wright, Q. (1983). *A Study of War.* Chicago: University Of Chicago Press.

Wyman, L. C. and C. Kluckhohn (1938). *Navaho Classification of Their Song Ceremonials.* Menasha: American Anthropological Association.

Xin, K. and J. Pearce (1996). Guanxi: Connections as Substitutes for Formal Institutional Support. *Academy of Management Journal 39*, 1641–1658.

Yan (2006). From Made in China to Serviced in China. Online: `http://english.ccpit.org/Contents/Channel_410/2006/1031/15647/content_15647.htm` [11.02.2008].

Yang, V. and L. Ehrichs (2007). The Professionalism of Judges: Education, Salaries and Career Structure in Asia. In: *Global Corruption Report 2007.*

Corruption in Judicial Systems, pp. 48–55. Cambridge: Cambridge University Press.

Yeh, R. (1988). On Hofstede's treatment of Chinese and Japanese values. *Asia Pacific Journal of Management 6*(1), 149–160.

Yeung, I. Y. and R. L. Tung (1996). Achieving business success in Confucian societies: The importance of guanxi (connections). *Organizational Dynamics 25*(2), 54–65.

Yong, K. (2003). Culture Issues in Taiwan's Civil Aviation Community. Online: `http://www.itsasafety.org/data/2003/Culture_study_in_Taiwan.doc` [19.6.2008].

Yum, J. O. (1994). The Impact of Confucianism on Interpersonal Relationships and Communication Patterns in East Asia. In: L. A. Samovar and R. E. Porter (Eds.), *Intercultural Communication: A Reader* (Seventh ed.)., pp. 75–87. Belmont: Thomson Wadsworth.

Zarnekow, R., W. Brenner, and H. H. Grohmann (Eds.) (2004). *Informationsmanagement. Konzepte und Strategien für die Praxis*. Heidelberg: dpunkt Verlag.

Zhang, X. (2004). Can Rural China Keep Up?. Online: `http://www.chinatoday.com.cn/English/e2004/e200406/p10.htm` [20.07.2008].

Zhao, Y. (1999). Labor Migration and Earnings Differences: The Case of Rural China. *Economic Development and Cultural Change 47*(4), 767–782.

Zhu, Z., K. Hsu, and J. Lillie (2001). Outsourcing – A Strategic Move: The Process and the Ingredients for Success. *Management Decision 39*(5), 373–378.

Zittrain, J. and B. Edelman (2003). Internet Filtering in China. *IEEE Internet Computing 7*(2), 70–77.