Analyse & Kritik 26/2004 (© Lucius & Lucius, Stuttgart) p. 48–62

Hans-Werner Bierhoff/Bernd Vornefeld

The Social Psychology of Trust with Applications in the Internet

Abstract: Three levels of trust as a social psychological construct are delineated: trust in a specific person (relational trust), trust in people in general (generalised trust) and trust in abstract systems. Whereas much research is available on relational trust and generalized trust, much less is known about trust in systems. From theory and research several assumptions are derived which are related to the development of trust in the Internet. For example, the reliability of information technology is assumed to be directly related to the development of trust in the Internet. In addition, it is assumed that in situations in which it is hard to verify the justification for trust, people construct subjective beliefs which represent a transformation of relational trust into system trust. Applications of these assumptions for strengthening the trustworthiness of the Internet are discussed.

1. Introduction

The Internet age needs trust. The Internet presumably is the most visible and most significant representative of the knowledge society encompassing information, knowledge, and the intelligence of systems (Bleicher 2003). An example is the cooperation of work groups in virtual organisations which are linked, distributed organisational units (Krystek 2003). "Trust gains significance as an organisational principle in the transition to the knowledge society." (Bleicher 2003, 341)

At the same time the Internet age has elicited a strong need for security and control, respectively. This seems to be a contradiction, because if people would have sufficiently strong trust, there would be no need to exert control (Auhagen 2003). Individuals seek security in Internet applications because trust is often not justified. The more security is guaranteed, the easier it is to have trust. This idea is the focus of Perc and Schneider's (2000) theoretical reasoning: A perceived risk to suffer a loss is counterbalanced by information which reduces the risk. Such information includes contracts, system trust, and more specific trust.

Although the Internet is a technical system with strict, built-in security measures, it is managed, maintained, and used by humans and therefore will never be able as a system to guarantee perfect security. Baurmann (2003, 337) notes in this context, "that institutions cannot be created 'out of nowhere' without a basis of personal trustworthiness". Complex technical systems are subject to a

multitude of potential sources of error: software errors, design errors, and service errors.

Many activities of Internet users presuppose personal and/or system trust. Three examples illustrate this point: Firstly, persons who exchange intimacies during a chat without knowing the identity of the other party assume that their chat partner is being truthful about his or her gender and age. Another example is an Internet user who downloads a software program from a server without knowing whether at this opportunity an additional program may be stealing its way into his or her operating system, which will ask him or her to call up a specific Internet page again and again in the future ('trojans'), or which attempts to destroy data (viruses), or which redirects the Internet connection to an expensive provider (dialers). Thirdly, the use of computer mediated communication by scientists is limited by doubts with respect to the reliability of information and by the expectation that personal interests are harmed by sharing information with others, respectively (Kling/McKim 2000).

Therefore, the question emerges whether social-psychological trust research is able to contribute to an understanding of the use of the Internet. Which levels of trust have to be taken into account? Do Internet users implicitly make a compromise between trust and security, in order to communicate conveniently on the one hand and securely on the other hand? When are users convinced that the Internet is reliable or specific online services or persons with whom they electronically communicate with are trustworthy? Which possibilities exist to constrain the dangers of misuse of the Internet?

To answer these questions, we analyse in more detail the social psychology of trust in the first section. We differentiate three levels of trust, which we refer to in the following: specific trust, generalized trust, and system trust. In the second section we consider the consequences of trust insofar as they are relevant for the Internet. In this context we emphasize the development of techniques which increase security in the Internet.

2. Social Psychology of Trust

Social psychological research has dealt with the topic 'trust' for more than 40 years. Originally, trust was considered in the context of factors which were assumed to facilitate or inhibit cooperation in groups. Later, other areas of application were taken into account, e.g. trust in teachers and trust in doctors. In a bibliography, which takes publications on trust until 1997 into account, 797 contributions were found (Schweer 1998). In addition, recent overviews (Kramer 1999; Schweer 2003) clearly show that trust is still in the centre of attention of social psychologists.

Trust and risk are complementary terms in social relations. An emphasis on risk is generally based on mistrust, whereas trust is associated with less doubts about security. Those who trust others do not look for high security before they act.

Trust is related to reliability of information which may reduce insecurity and

risk. This is visible in the following definition: Trust is a "reliance upon information received from another person about uncertain environmental states and their accompanying outcomes in a risky situation" (Schlenker/Helm/Tedeschi 1973, 419).

Individuals make concessions to security and safety because social reality is highly complex. Effective action is only possible if the person succeeds in reducing social complexity. This is exactly the function of trust (Luhmann 1973): Objective uncertainty is transformed into subjective certainty.

What the definition of trust does not address is the question from which sources the trustworthiness of a person is derived. The goal/expectation theory of individual and simultaneous cooperation (Pruitt/Kimmel 1977) was developed as a partial answer to this question. The assumption that another person is trustworthy is derived from several sources:

- The other person has cooperated with others in the past.
- The actor has been involved in a conflict situation with the other person in the past, in which a cooperative solution was found.
- The other person communicates that he or she has the intention to cooperate.
- It is plausible to assume that the other person has come to the insight that his or her own interests are best served by cooperating because a mutual dependence is given.

Therefore, if no direct experience from the past is available as a standard of judgment to rely on, the possibility exists that the target person collects information from third persons, who have made own experiences with the other person in conflict situations which are evidence for his or her trustworthiness.

A variant of trust which is especially significant in the Internet is system trust which is associated with abstract systems, one of which is the Internet. System trust is a relevant factor because the technical processes which make up the Internet are in general not transparent for the user (Krystek 2003). Giddens (1991) considers the formation of such abstract systems a central characteristic in the development of modern societies (cf. Fiedler 2003).

Instead of receiving information about local events through direct personal perception, in the Internet age persons increasingly use communication channels, which do not stem from direct experience, as a source of information. Computer-mediated communication among researchers in different scientific disciplines is an example (Matzat 2002). Giddens (2001, 680) comments in this context: "Trust in other people used to be based in the local community. Living in a more globalised society, however, our lives are influenced by people we never see or meet, who may be living on the far side of the world from us."

As we have seen, trust overcomes risk and uncertainty in interpersonal relationships. Trust may be disappointed or confirmed depending on whether the other person misuses or respects it. Trust refers to the relationship between

two people and therefore is called 'relational trust' (Jones/Couch/Scott 1997) or 'specific trust' (Buck/Bierhoff 1986).

Specific trust is 'the expectation that the other will cooperate' including the perception of the other's attitudes and personality traits (Pruitt/Kimmel 1977, 375) which are assumed to facilitate cooperation. Specific trust may be misused. Therefore, people are especially sensitive to cues which indicate that others misuse trust and as a consequence are not trustworthy. The basis for this sensibility may have originated during the evolution of social behaviour (Voland 1998). Nevertheless, people are willing to develop trust (and in a sense they are forced to develop trust). With respect to the assessment of specific trust, an optimistic pattern was found (Bierhoff 1995): People are easily persuaded to form trust. In addition, empirical results indicate that the assessment of specific trust at two measurement points toward another person is quite stable. This shows that the impression formation which is based on the first encounter has a certain stability across time. It is obviously less influenced by moods than by the variables of the other person. If these variables stay constant, specific trust will not change much either.

From these results the conclusion is drawn that a certain level of trust toward an interaction partner tends to persevere after impression formation has taken place. Presumably this tendency is even stronger in the Internet because the communication channels are impoverished compared to a face-to-face-interaction. Therefore, the first impression which determines the initial trust level might have far-reaching consequences. This tendency might be reinforced in the Internet because the other person is able to carefully plan and manipulate his or her appearance to a greater extent than is possible in everyday interactions. Only if a person appears to be inconsistent or contradictory, the trust level will be instable or may even break down altogether.

Specific trust is an interpersonal resource which might have positive effects on communication. For example, persons who express trust in their interaction partner are likely to rely on prosocial coping strategies instead of antisocial coping strategies (Buchwald/Schwarzer 2003). The mediating role of specific trust on the facilitation of interpersonal communication in face-to-face interaction which was demonstrated by Buchwald (2003) is likely to extend to Internet communication.

Specific trust is different from 'generalized trust', which is defined "as an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon" (Rotter 1967, 651). Generalized trust is not the same as naivety or gullibility (Rotter 1980). Even people who are characterized by a high level of generalized trust are sensitive to betrayal by others. In addition, generalized trust has many favourable consequences for the 'high believer'. Empirical results show that high believers are attractive for others, they are preferred as friends by others, and express more happiness.

In the following, the issue of generalized trust is discussed in more detail. It is measured by statements like

> "In dealing with strangers one is better off to be cautious until they have provided evidence that they are trustworthy."
>
> "Parents usually can be relied upon to keep their promises."
>
> "Most elected public officials are really sincere in their campaign promises."

Amelang, Gold and Külbel (1984) distinguish four dimensions of generalized trust: trust in official institutions, trust in other people in general, trust in experts, and trust in the correspondence between verbal statements and real actions to which they refer. This dimensional classification of generalized trust is only partially applicable to the Internet. But the dimension 'trust in experts' might be relevant for the use of information and communication technologies, the installation of which is dependent on expert knowledge. The higher the trust in experts, the more willing a person might be to demonstrate trust in the Internet. This assumption waits for empirical validation.

In addition, the question whether the assumption of a specific dimension of Internet trust is viable is an issue of further research. Presumably, an independent dimension of Internet trust is more likely to develop if the Internet in its social representation is more distant from other communication services like radio, TV, or phone. On the other side, if radio, TV, or phone become increasingly available on the Internet, the distinction between Internet trust and other dimensions of generalized trust may become unnecessary.

Be this as it may, empirical research shows that the aforementioned dimensions of generalized trust are positively correlated with each other. For example, if a person expresses stronger mistrust in experts, the mistrust in the correspondence between verbal statements and real actions is also stronger. The content-specific differentiation of several areas of generalized trust proves to make sense if statements about the expectancies of a person in a specific domain are aimed at. From this viewpoint it seems desirable to measure generalized Internet trust by developing an appropriate inventory.

The distinction between the specific and the generalized level of trust is of great significance because both forms of trust are independent of each other. That is, the level of generalized trust does not have any implications on specific trust (Buck/Bierhoff 1986). The correlation between specific and generalized trust is about zero. This zero correlation points out that specific trust is not a derivation of generalized trust (Buck/Bierhoff 1986). Applied to the Internet, this means that the level of trust in experts, for example, will be almost completely independent from the trust which a person who participates in a chat room has toward a specific chat partner. Here the limitations of the measurement of generalized trust are clear. Even if generalised trust toward the Internet is measured, it is presumably no reliable basis for predicting trust in a specific chat partner.

The third type of trust is named system trust which is defined as "having confidence in 'abstract systems' " (Giddens 2001, 680). It is possible to distinguish different facets of system trust (Büssing/Broome 1999): One facet of system trust is that confidential information is treated confidentially and that

the participant believes that system security is guaranteed. Another aspect is that the reliability and speed of information transfer is trusted in. A third aspect is that the information and communication technology functions reliably.

These facets may be summarized under the heading 'socio-technical system trust' because it is related to technical and social structures of an organisation. Statements which were developed to measure socio-technical system trust include:

> "One can be sure that information sent within the organisation reaches the addressee."
>
> "One can depend on the correct functioning of information and communication technology."

The last item does not directly address trust in Internet technology, but it can be used as a model for formulating statements to assess Internet trust, for example:

> "One can depend on the correct functioning of the Internet."

The development of a questionnaire measuring trust in the Internet as an abstract system is an important prerequisite for research in this area. To illustrate how important the issue of system trust in the Internet is we describe the structure of the Internet in more detail. The Internet structure is so complex that even experts are not knowledgeable about all of its facets. Computer laypersons consider it a black box most of the time. The functioning of the Internet is dependent on the error-free coordination of various hardware and software components. To describe the functionality of network systems, several models are available: The most well-known models are the ISO (International Standards Organization), the OSI-layer model (Open Systems Interconnection), and the layer model of the US defence department which is the basis of the Internet (DoD). The communication process is subdivided into seven layers, each of which has its own tasks and its own protocols (see Table 1). A protocol is defined as a set of agreements referring to how data are transferred from one program to another. Each layer may use different protocols.

OSI-Model	***DoD-Model***	***Protocols***
7 Application layer	4 Application layer	Telnet, FTP, SMTP, TFTP, HTTP, ...
6 Presentation layer		
5 Session layer		
4 Transport layer	3 Host-to-host layer	TCP, UDP, ..
3 Network layer	2 Internet layer	IP, ICMP, ARP, RARP, ...
2 Data-link layer	1 Network access layer	Ethernet, Token Ring, FDDI, ...
1 Physical layer		

Table 1: Comparison between the layer models of OSI and DoD (cf.http://www.wi1.wiso.uni-goettingen.de/pa/reco/kompetenz/schichtenmodell/1.htm)

If data are sent, each layer gives the data plus own protocol information, the so-called 'header', to the next lower layer. The protocol information reveals who has sent the data and who is the receiver, which route the data are supposed to take during transference, how they are expected to be worked off or how they are expected to be treated by the receiver. On the receiver side, the layers are run through in reverse order. Each layer works off protocol information which is targeted for it, removes it, and sends the remaining data to the next higher layer until the application layer is reached.

Attacks and defence measures are principally possible at each layer. From the point of view of the user, the most important layer which is under his or her control is the application layer. Many programs ask for access to the Internet, justified or unjustified. In this context, desktop firewalls have an important security function. At the level of the transport layer, network firewalls apply which frequently are integrated into the router.

System trust is only marginally connected with organisational bonding and work commitment. Instead, these are more strongly influenced by personal trust (Büssing/Broome 1999). An example for the combined effect of level of specific trust and level of system trust is buying goods in the Internet (eBay, Döring 2003). The willingness to bid in such an auction becomes greater as the reputation of the agent (system trust) and perceived reliability of the seller of the item (specific trust) increase. The importance of trust and distrust, respectively, becomes particularly visible when the buyer must first pay for the goods before receiving them. This type of trust building (or distrust building) in eBay transactions has not yet been examined in any great detail. However, one can assume that agent reputation can be heightened through specific measures (Perc/Schneider 2000). Such reputation-enhancing techniques are very important in the Internet because they can help lower the risks involved in such transactions (cf. other contributions to this volume).

3. Selected Techniques Which Increase Security in the Internet and Consequences For Trust

In the following we discuss techniques which increase security in the Internet and how they affect trust of the user. In which ways can trust influence an individual's use of the Internet? A first consideration is based on the knowledge that trust is connected with cooperation (Deutsch 1958; Pruitt/Kimmel 1977). If there is high trust in the cooperative attitude of others, then the individual will cooperate more readily than if trust is low. The prerequisite for this, however, is that the person is at all interested in cooperation. Transferring this to the Internet one can expect that high system trust increases the readiness to make new contacts, to send information, and to use new means of communication.

Trust is one prerequisite for using the Internet because there is no way to ensure perfect security, as illustrated by numerous examples for security breaches which have occurred in the past. From this perspective, an interesting question is how high the person's trust in the Internet should be under the premise that

we are dealing with a system in which conflicting interests of different users exist. Presumably, such a system functions in an optimal way if there is a moderate degree of trust (cf. Gamson 1968). If individual system users place too much confidence in the system, they are being careless because the danger of intentional disturbances or disruptions as side-effects of advertisements, for example, is omnipresent.

Furthermore, it appears sensible to vary the degree of trust depending on who is the sender. If there is no previous knowledge of the sender, a higher degree of mistrust is appropriate than if the sender has already proven to be trustworthy in the past (cf. goal/expectation theory). However, the fact that the sender is known is no guarantee for receiving reliable information. Deliberate manipulations by third parties can distort messages from senders or initiate messages from text fragments stored on the sender's computer.

In which cases will the degree of subjective trust be high? Trust will be particularly high if control mechanisms, the effectiveness of which the user is completely convinced (e.g. anti-virus software), are directly available and easy to use.

Another example is online banking. The bank bears the costs and responsibility of ensuring secure transactions, whereas the customer does not have to invest anything, with the possible exception of having to use a specific browser or add-on program. However, if the browser or add-on is a proprietary product which runs only on a special operating system, then the necessary time and effort for the user can increase tremendously. Trust is an important prerequisite for using this system, which uses a password to ensure security. The procedure a person follows in online banking which is designed analogously to using an ATM (Automated Teller Machine) presumably increases the subjective confidence of the bank customer. This makes it more easy for the customer to entrust himself or herself to the online banking system, even though large amounts of money may be involved. This can lead to exaggerated ideas about the security level accompanying each transaction.

One way to heighten security in the Internet is the preferred use of information stemming from certified senders. A number of private companies (e.g. VeriSign) sell certificates to businesses, which in turn can resell these certificates to others, or to end users (e.g., web businesses). If the browser of the addressee receives the certificate, a verification of the sender is started. This inquiry is directed to the original certification agency; if it is confirmed, then the certification is accepted. If not, then the browser issues a warning. In general, a certificate contains an encryption code, which ensures that the addressee receives the unchanged, original message.

Extreme mistrust of the Internet limits communication possibilities. However, this mainly applies to persons who do not have much knowledge about data transmission in the Internet. More knowledgeable persons can encode their messages or use alternative operating systems, such as Linux. On the other side, simply using another operating system such as Linux is no guarantee for more security. This functions only as long as there are less viruses for the Linux op-

erating system than for Windows (in other words, as long as the vast majority of users use the Windows platform).

Another important question is how much control over his or her computer does the individual have (i.e., company computer or private computer). In any case, trust interacts with the system knowledge of the user (about the operating system, application software, and Internet technology).

Incidentally, the comparison of operating systems shows that there are different ways to deal with the complexity of computer-supported communication. Windows simplifies the processes in so far as the user is not directly confronted with system administration processes. However, with Ctrl+Alt+Del a user can activate the task manager, which displays information about running processes, memory usage, and system variables (handles, threads). In contrast, Linux automatically sends many process status messages to the user. When Linux starts up, a lot of information is displayed concerning the status of the start-up process. (This information is also accessible in Windows if the user opens the respective file which documents the start-up process.) Naturally these messages only make sense if the user knows what they mean, which often is not the case.

In the case of limited computer knowledge, the perception of safety is rather an illusion of security than an objective judgement. If, for example, a virus scanner is used, this will increase subjective confidence. However, this heightening of subjective security can be a complete illusion if the virus scanner is outdated, because it is no longer able to identify all the latest viruses.

Presumably, a user 's subjective distrust is primarily connected with past experiences of data loss, virus attack, or computer crashes, in other words, relevant negative prior experiences. If harm is caused, it makes a difference if the damage was restricted to the user's work area or if his or her reputation was harmed. The latter type of damage should have particularly strong negative effects on the user's trust.

Finally, we will turn to techniques that heighten security, so that the user must muster up less trust in order to have confidence in the system's reliability (in the sense of trust readiness as defined by Perc/Schneider 2000). These methods are based on a highly reliable verification process of the identity of server and client, in order to prevent third party attacks (i.e., man-in-the-middle attacks). One example is the use of the Kerberos system; although it ensures a high degree of security in the Internet, it is implemented only rarely. Besides the server of the sender, this system requires two further servers, which provide for authentication and authorization. Authentication confirms the identity of the user. However, at present the use of digitally signed messages is more the exception than the rule. In addition, there is the problem that others may be able to read the message. This problem can be dealt with by using an encryption code. Authorization means that a confirmation is given that the client is allowed to access the server. Numerous communications are exchanged between the respective servers and the sender (sending the session encryption code etc., ensuring that the authentication by the specified server takes place, etc.) in order to guarantee the desired level of security of information exchange between client and server.

Authentication and authorization are components of a system, which allow a verification of identity (Döring 2003, 547). In order to eliminate virtually all sources of risk, extensive preventive measures are necessary, which most clients are not willing to undertake, even if they theoretically have the knowledge to protect themselves. This is so because excessive resources must be expended (i.e., time and money) in order to realize so high a degree of Internet security that the client would only have to muster up a minimal degree of trust in the system.

Less sophisticated methods, such as those employed in online-banking and based on the Secure Socket Layer (SSL) (often symbolized by 'https' in the address line), do not completely rule out attacks by third parties (man-in-the-middle attack), because it is not possible to guarantee that the recipient is actually interacting with the intended server (however, after the attack, one can trace back where the attack came from).

In many Internet services, usually also in sending and receiving email messages, the users alone are responsible for their security. More often than not this means that no precautionary measures are taken. For email, for example, reliable methods such as PGP (Pretty Good Privacy, which is one of the most widely distributed public key encryption tools) or GPG (Gnu Privacy Guard, which is an open source implementation of PGP) have existed for years. Their use, however, requires basic knowledge of encryption methods.

3.1 Public Key Encryption

Classic methods for encryption use only one key for encryption, which the sender uses to encrypt the message. In order
to decrypt it, the receiver needs the very same key. Thus, this key must be given to the receiver in such a way that no other person can gain access to it. If somebody else receives access to the key, this method of encryption is worthless.

The use of so-called public keys can be a solution. Public Key Encryption is a concept using two keys. One key is a public key that can be distributed through all sorts of electronic channels and may be obtained by any person. The other key is the private key. This key is secret and cannot be accessed by others; it is only available to the owner. If the system is well implemented, the secret key cannot be derived from the public key. The sender encrypts the message with the public key belonging to the receiver. Decryption is done with the secret key of the receiver.

Crucial in this concept is that the secret key remains a secret; it should not be disclosed or become accessible to anyone else but the owner. Also, it is very unwise to use GPG or PGP over telnet (you should consider avoiding the use of telnet altogether because of the high security risks).

3.2 Digital Signatures

In order to assure that a message was really sent by the alleged sender, the concept of digital signatures was developed. As the name says, a message is digitally signed by the sender. This signature proves that the message is authentic. This

technology can reduce the risk of Trojan horses (e.g., a message that claims to be a patch for a specific problem but actually contains a virus or destroys data on the computer). Also, information or data can be verified as coming from a legitimate source and thus be regarded as correct.

A digital signature is made through a combination of the secret key and the text. Using the senders' public key, the message can be verified. Besides checking if the message stems from the original sender, the content is also checked. Thus, the receiver of the message knows that it really came from the original sender and that it has not been changed during data transmission.

3.3 Web of Trust

A weak point of public key algorithms is the distribution of public keys. A user could bring a public key with a false user ID into circulation. If messages are made with this particular key, the intruder can decode and read the messages. If the intruder passes it on this attack goes unnoticed.

The PGP solution (the same applies to the GPG solution) exists in signing codes. A public key can be signed by other people. This signature acknowledges that the key used by the UID (User Identification) actually belongs to the person it claims to be from. The user of GPG must decide for himself or herself how far trust in the signature is warranted. You can consider a key as trustworthy if you trust the sender of the key and know for sure that the key really belongs to that person. Only if you can trust the key of the signer, you can also trust the signature. To be absolutely sure that the key is correct, you have to compare the fingerprint over reliable channels.

3.4 Trust Centres

A trust centre is a certification authority in accordance with the digital signature act.

In order to ensure that a certain public electronic key belongs to a certain person or institution within a public key infrastructure (PKI, a highly trusted and independent third party must have reliably examined the assignment beforehand. Thus, this third party can vouch for the identity of the key owner.

This trusted third party is the so-called trust centre, which functions as a kind of 'electronic notary'. After the identification of a person, e.g. by identity card, the trust centre issues a digital certificate to confirm that a specific electronic key belongs to a specific certificate owner. The certificates are stored in a secure electronic database, which is always accessible so that another person can check the validity of the certificate and the authenticity of the owner at any time.

The certificates are generated by the trust centre using so-called certificate servers and stored on 'directory servers'. For security reasons a certificate is only valid for a specific length of time. If the certificate expires or is invalidated, it will be removed from the directory server and stored in a 'CRL' (Certificate Revocation List), which is always accessible. With the help of this revocation list, one can check whether a certificate was valid at a certain time or not.

In order to ensure the credible and reliable operation of a trust centre and to

guarantee—if necessary—that a digital signature is legally binding, the German signature act has set up strict standards governing the establishment and operation of a legally recognized certification authority. In Germany the Institute for Telematics is the institution, which has the task to ensure compliance with legal regulations and watch over their technical implementation.

Why is PKI not yet widely implemented? Some reasons are:

- It is more complicated than originally believed, therefore it will take some time until this technology is generally accepted.
- Users are not aware of possible risks, in other words, they place too high trust in the system.
- A PKI could prove to be bothersome in the sense that a boss cannot tell his secretary to sign his name in his absence.
- There is (covert) political resistance.
- The 'killer application' is missing.
- The necessary security infrastructure cannot be implemented on insecure computers, which often applies to standard PCs.

3.5 Virtual Private Networks

Businesses are well-advised to accommodate the needs of remote employees. An elegant method to mitigate many potential risks involved in data transfer is the use of a Virtual Private Network (VPN), which tunnels all electronic communication between distant corporate network sites through the Internet.

The latest technical developments promise that sophisticated authentication and encryption procedures will ensure almost completely tap-proof data transmission through the Internet, if these are carefully implemented. In the following we will address VPNs in more detail because they are becoming increasingly popular (since these networks provide high security against data tapping and message manipulation). Basically, the main objective is safe data access, for example, for remote workers. The heart of the technique is the creation of a tunnel with an entrance and an exit. All data between the two ends of the tunnel is encrypted, so that an eavesdropper hears nothing but white noise. Currently many businesses are expanding their private networks to 'virtual private networks' by tunnelling the Internet.

Virtual private networks are attractive because of their low cost, since they do not require their own physical infrastructure. Dedicated lines, call-in ports in the own network, call-back Internet access, own radio-controlled or cable connections between company branches or between branch and teleworkers are no longer needed. A normal Internet connection for all networkers is sufficient. Depending on how broad the band is or how long online time is, one can choose between modem, ISDN, DSL, or LAN to access the Internet. The actual data transmission takes place over the public Internet.

Since the Internet is a vulnerable space, in which every user must fear his or her data being manipulated or spied upon, the 'normal' use of the Internet would be too risky. Conventional encryption methods on the protocol layer or application layer necessitate a high degree of attention of all involved parties. The principle underlying the VPNs simplifies safe data communication by transferring the entire data stream in encrypted form between the users of the network. VPNs are—so to speak—a network in a network, which remains transparent for applications as well as users. In simple words, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users.

4. Perspectives For Further Research

Research on 'Trust in the Internet' is just beginning. A number of research tasks are pressing and promising at the same time:

- the development of questionnaires to measure psychological constructs in general (e.g. personality dimensions; Hertel/Naumann/Konradt/Batinic 2002) and trust in the Internet more specifically (cf. Batinic/Reips/Bosnjak 2002);
- the development of methods and instruments for experimentation in the Internet (see Reips 2002);
- the application of devices for risk and security assessment in the Internet and the supplement of technological approaches by psychological perspectives on interpersonal and system trust;
- the relationship between trusting behaviour on the one hand and perceived reliability of information on the other hand in computer-mediated communication (cf. Matzat 2002).

The Internet is a new medium of communication which offers a large increase in information exchange among participants. But it is not without hazards. A continuing task will be to find the optimal balance between gullibility and paranoia. This balance is a matter of individual preferences and of organisational climate, respectively. At the same time, it is an empirical question how the balance between trust and distrust relates to successful use of the Internet.

Bibliography

Amelang, M./A. Gold/E. Külbel (1984), Über einige Erfahrungen mit einer deutschsprachigen Skala zur Erfassung zwischenmenschlichen Vertrauens (Interpersonal Trust), in: *Diagnostica 30*, 198–215

Auhagen, A. E. (2003), Zum Wesen von Vertrauen, in: *Erwägen, Wissen, Ethik 14*, 333–335

Batinic, B./U. D. Reips/M. Bosnjak. (eds.) (2002), *Online Social Sciences*, Seattle

Baurmann, M. (2003), Kontrolle ist gut, Vertrauen ist nötig, in: *Erwägen, Wissen, Ethik 14*, 335–337

Bierhoff, H. W. (1995), Vertrauen in Führungs- und Kooperationsbeziehungen, in A. Kieser/G. Reber/R. Wunderer (Hg.), *Handwörterbuch der Führung*, Stuttgart, Spalten 2148–2158

Bleicher, K. (2003), Vertrauen gewinnt als Organisationsprinzip beim Übergang in die Wissensgesellschaft an Bedeutung, in: *Erwägen, Wissen, Ethik 14*, 341–344

Buchwald, P. (2003), The Relationship of Individual and Communal State-Trait Coping and Interpersonal Resources as Trust, Empathy, and Responsibility, in: *Anxiety, Stress and Coping 16*, 307–320

— /C. Schwarzer (2003), The Exam-Specific Strategic Approach to Coping Scale and Interpersonal Resources, in: *Anxiety, Stress and Coping 16*, 281–291

Buck, I./ H. W. Bierhoff (1986), Verlässlichkeit und Vertrauenswürdigkeit: Skalen zur Erfassung des Vertrauens in eine konkrete Person, in: *Zeitschrift für Differentielle und Diagnostische Psychologie 7*, 205–223

Büssing, A./P. Broome (1999), Vertrauen unter Telearbeit, in: *Zeitschrift für Arbeits- und Organisationspsychologie 43*, 122–133

Deutsch, M. (1958), Trust and Suspicion, in: *Journal of Conflict Resolution 2*, 265–279

Döring, N. (2003), *Sozialpsychologie des Internet*, Göttingen

Fiedler, M. (2003), Über Systemvertrauen und Vertrauenswächter, in: *Erwägen, Wissen, Ethik 14*, 348–349

Gamson, W. A. (1968), *Power and Discontent*, Homewood

Giddens, A. (1991), *Modernity and Self-Identity*, Oxford

— (2001), Sociology (4th edition), Cambridge

Hertel, G./S. Naumann/U. Konradt/B. Batinic (2002), Personality Assessment Via Internet: Comparing Online and Paper-and-Pencil Questionnaires, in B. Batinic/U. D. Reips/M. Bosnjak (eds.), *Online Social Sciences*, Seattle, 115–133

Jones, W. H./L. Couch/S. Scott (1997), Trust and Betrayal. The Psychology of Getting Along and Getting Ahead, in R. Hogan/J. Johnson/S. Briggs (eds.), *Handbook of Personality Psychology*, San Diego, 465–483

Kling, R./G. McKim (2000), Not Just a Matter of Time: Field Differences and the Shaping of Electronic Media in Supporting Scientific Communication, in: *Journal of the American Society for Information Science 51*, 1–13

Kramer, R. M. (1999), Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions, in: *Annual Review of Psychology 50*, 569–598

Krystek, U. (2003), Vertrauen und virtuelle Unternehmungen: Scheitert Vertrauen als Organisationsprinzip an neuen Organisationsformen? in: *Erwägen, Wissen, Ethik 14*, 362–364

Luhmann, N. (1973), *Vertrauen*, Stuttgart

Matzat, U. (2002), Academic Communication and Internet Discussion Groups: What Kinds of Benefits For Whom? in B. Batinic/U. D. Reips/M. Bosnjak (eds.), *Online Social Sciences*, Seattle, 383–402

Perc, P./S. Schneider (2000), *Vertrauen im Internet*, Frankfurt

Pruitt, D. G../M. J. Kimmel (1977), Twenty Years of Experimental Gaming. Critique, Synthesis and Suggestions For the Future, in: *Annual Review of Psychology 28*, 363–392

Reips, U. D. (2002), Theory and Techniques of Conducting Web Experiments, in B. Batinic/U. D. Reips/M. Bosnjak (eds.), *Online Social Sciences*, Seattle, 229–250

Rotter, J. B. (1967), A New Scale For the Measurement of Interpersonal Trust, in: *Journal of Personality 35*, 651–665

— (1980), Interpersonal Trust, Trustworthiness, and Gullibility, in: *American Psychologist 35*, 1–7

Schlenker, B. R./B. Helm/J. T. Tedeschi (1973), The Effects of Personality and Situational Variables on Behavioral Trust, in: *Journal of Personality and Social Psychology 25*, 419–427

Schweer, M. K. W. (1998), *Vertrauen*, Landau

— (2003),Vertrauen als Organisationsprinzip: Vertrauensförderung im Spannungsfeld personalen und systemischen Vertrauens, in: *Erwägen, Wissen, Ethik 14*, 323–332

Voland, E. (1998), Die Natur der Solidarität, in K. Bayertz (Hg.), *Solidarität*, Frankfurt, 297–318