

**Prof. Dr. iur. Bernd Lutterbeck**  
**Technische Universität Berlin**  
**Institut für Wirtschaftsinformatik**

**Trusted »», trustworthy»», treacherous»» oder controlled»»  
computing? Gedanken zu einer gesellschaftlich  
notwendigen Debatte**

Symposium «Trusted Computing Group, veranstaltet vom  
Bundesminister für Wirtschaft und Arbeit  
Dinner-Speech am 2. Juli im Museum Hamburger Bahnhof Berlin

**Prolog**

Es gibt nur eine Gewissheit unter Menschen: den Tod.

Alles andere ist ungewiss.

Die Dinge zwischen den Menschen sind immer ungewiss.

Warum schlagen sich Menschen nicht dauernd die Köpfe ein?

Weil sie sich vertrauen.

Warum vertrauen Menschen sich?

Wer die Antwort theologisch geben will: Weil sie Gott vertrauen.

Wer eine eher ökonomische Antwort bevorzugt – schließlich bereiten wir  
uns auf ein Essen vor, das der Bundesminister für Wirtschaft sponsert:

Weil sie gelernt haben, dass Kooperation eine vorteilhafte Strategie ist.

Kooperation gelingt nicht immer – das zeigen die vielen Kriege und der  
andauernde Terrorismus.

Kooperation muss auch nicht moralisch hochwertigen Antrieben  
entspringen: Je «teurer» es ist zu lügen, desto eher ist die Annahme  
berechtigt, dass die Kommunikation der Wahrheit entspricht, umso eher  
stellt sich Vertrauen ein. (Rudinger)

In vielen Situationen muss man Kommunikationen glauben: Weder kann  
man den Wahrheitsgehalt von Informationen überprüfen, noch erhält  
man Gewissheit über den Partner der Interaktion.

Risiko und Vertrauen gehören also zusammen, sind Korrelate.

Dieses alles kann der Dichter Max Frisch in einem einzigen Satz  
zusammenfassen:

«Jeder Versuch sich mitzuteilen, kann nur mit dem Wohlwollen der  
anderen gelingen.»

Jetzt habe ich so was wie eine Messlatte aufgebaut. Die müsste man überspringen, wenn man meinem Thema gerecht werden wollte: Wer sich nicht gehörig in Theologie, Psychologie und Ökonomik, besonders in ihrem gegenwärtig so aussichtsreichen Zweig der empirischen Wirtschaftsforschung umgeschaut hat, sollte den Wettbewerb eher meiden. Und natürlich ahnen Sie, dass im Hintergrund das Recht auf der Lauer liegt.

Keine Bange: Ich weiß, was sich gehört.

Zur Sicherheit habe ich meinen Freund Alfred gefragt: «Alfred, jetzt sag mir doch mal, wie muss ich ein – eine – einen «Dinner-Speech» halten?» Alfred, das sollten Sie wissen, nimmt regelmässig an Vorstandssitzungen des größten deutschen Konzerns teil.

Keine Sekunde hat er gezögert. Wie aus einer Pistole kam die Antwort:

- Zwei Witze
- Eine Message
- Und weniger als 15 Minuten.

«Alfred, Dein Wort in Gottes Ohr!»

Einen Witz bin ich jetzt schon los geworden.

Auch meine Botschaft ist klar: Sie müssen sich auf die Einsicht vorbereiten, dass das Thema «TCPA» eigentlich mit Computern gar nichts zu tun hat.

Ich kann Sie aber trotzdem noch nicht zur Speise entlassen. Nachher verwechseln Sie diese Einsicht mit der Behauptung von Nikolas Carr, die er jüngst in der Harvard Business Review aufgestellt hat: IT-Investitionen, mithin auch Investitionen in IT-Sicherheit seien eh' sinnlos, weil sie keinen messbaren Ertrag brächten. (Betschon 2003)

Meine Botschaft ergibt sich aus drei Weisheiten:

- Der Weisheit der Römer: die Gleichheit
- Der Weisheit der Internet-Designer: end-to-end trust
- Der Weisheit des Marktes: Wettbewerb

## **Die Weisheit der Römer: Gleichheit**

Man kann nur definieren, was man verstanden hat.

Man wundert sich deshalb nicht, dass selbst die Marketinggenies diesseits und jenseits des Atlantiks noch immer nicht so genau wissen, worüber sie reden.

Ross Anderson hat mir deshalb aus der Seele gesprochen, wenn er in seinem Beitrag für die wissenschaftlich wichtige Konferenz «Economics and Information Security» im Mai 2003 nur die Abkürzung «TC» benutzt. Eine pfiifige Idee: Für jeden Geschmack etwas. Der Blick entscheidet. Und für den Alltagsgebrauch reicht es aus, sich den Unterschied von «trusted» und «trustworthy» so klar zu machen: Wenn ein Angestellter der NSA auf einer Toilette In Baltimore Washington International Airport beobachtet wird, wie er einem chinesischen Diplomaten «key material» verkauft, dann können wir ihn beschreiben  
«as `trusted` but not trustworthy`. (Anderson 2003)

Wenn etwas so schwierig wird, muss man es auf seine elementarsten Bestandteile reduzieren.

Wo muss man sie suchen?

Bei der Suche hat mir ein Beitrag von Dirk Kuhlmann außerordentlich geholfen, der bei den HP-Laboratorien in Bristol arbeitet. Dirk ist ein früherer Student von mir, ich darf ihn schon deshalb als Quelle heranziehen, «On TCPA» heißt sein Beitrag. (Kuhlmann 2003)

Wir brauchen «Trusted Platforms» schreibt er. Das Anliegen des Konsortiums sei grundsätzlich vernünftig, kann man von ihm lernen. Allerdings sei damit noch nichts gesagt über das Aussehen der Plattform. Natürlich weiß er, dass die TC eines Systems immer von der Reputation eines Besitzers, «owners» abgeleitet werden muss. Das zwingt dazu, sich der Umstände ganz einfacher Kommunikation zwischen Menschen zu vergewissern. Zur Lösung schwebt ihm vor, dass Modell des Vertrages auf das TC-Problem zu übertragen – ein «communication contract model». Eine interessante Idee: Wenn es schwierig und unübersichtlich wird, bedient man sich altbekannter Typen und rekonstruiert und von daher das Ganze. Man baut alles noch mal von vorne.

Ich glaube, dass Dirk Kuhlmann's Idee weiterführt.

Aber, lieber Dirk, ich muss Dich auf einen Fehler schon im ersten Satz Deines Beitrags hinweisen. Es sei vergleichsweise einfach, den Kontext der direkten Kommunikation zu erfassen.

Falsch! Es ist ganz schwierig.  
Hier der Beweis:



Sie sehen eine Schar von Freiwilligen. Künftige Rekruten.  
Alle ganz verschieden: Dicke, Dünne, 7 verschiedene Völker plus Römer.

Kelten, Ägypter, Engländer, Goten und was alles so rumläuft. 7 verschiedene Sprachen plus Latein.

Einfache Kommunikation?  
Bewahre, Dirk!

Und – was denken Sie?

Schmiedet der Dienst in der Armee sie alle sagen wir zu einer gemeinsamen Plattform zusammen?

Nein!

Hinterher ist alles wie vorher. Eine einzige Kakophonie.



Man sieht also:

Befehl und Gehorsam allein funktioniert nicht. Wirkt irgendwie lächerlich. Einfach draufschlagen funktioniert auch nur mit Zaubertrank und dann nur für wenige. Wie auch «Microsoft-Bashing» nicht wirklich etwas klärt.

Die Römer als praktisch veranlagte Leute wussten, dass sie eine praktische Lösung für das Kommunikationsproblem finden mussten. Sie erschufen ein Wunder, eines der größten kulturellen Wunder der Menschheit: Sie erfanden ein Recht: die Gleichheit der Menschen. Denn nur Gleiche können Verträge schließen. Und die Möglichkeit, Verträge zu schließen, reduziert die Komplexität der Kommunikation dramatisch.

Logisch gab es ein kleines Problem: Das Ganze war verordnet. Das Recht der Gleichen galt nämlich nur für die Nicht Römer. Ausländerrecht würden wir heute sagen. Bedingung dieser Gleichheit war also die Ungleichheit. (Tönnies 1990; Maine) Später übernahmen die Römer ihr Ausländerrecht als eigenes.

Damit war die wichtigste Bedingung für die Pax Romana erfüllt. Für die Europäer unter uns: Von diesem Zustand träumen die Menschen noch heute.

**Also:**

**Eine Plattform des Vertrauens setzt die Gleichheit der Kommunikationspartner voraus.**

## **Die Weisheit der Internet-Designer: end-to-end trust**

Das end-to-end-Argument: Ein Datenpaket soll ungehindert von einem Ort zum anderen gelangen können: Kein Platz für Zensoren, kirchliche oder politische Bedenkenträger, Fundamentalisten, Spinner, Kapitalansammlungen.

Die Stunde der Ingenieure. (Salzer/Reed/Clark 1984)

Alles Notwendige darüber hinaus muss Außen passieren, in den obersten Schichten. Der technische Kern muss von Regulierung verschont bleiben. Nach allem, was man heute weiß, hat dies die Innovationen, die durch das Internet ermöglicht wurden, fast revolutionär beeinflusst. Innovationen konnten entstehen, weil die vielen Nutzer dezentral entscheiden konnten. Sie haben die Gestalt des Netzes bestimmt.

Warum sollte für solche TC-Plattformen etwas anderes gelten?

Wieder: Vertrauen muss am Ende entstehen. Sicherheit ist eine Funktion der Interaktion von Menschen. Ein gutes Beispiel für dieses Funktionsprinzip ist eBay.

Es war eine wunderbare Leistung der Ingenieure, dieses Elementarprinzip menschlicher Kommunikation in technische Protokolle umzusetzen.

**Also:**

**Sicherheit entsteht durch Interaktion von Menschen – nicht ausschließlich, aber hauptsächlich.**

## **Die Weisheit des Marktes: Wettbewerb**

Die Römer wussten, dass man mit Verträgen Märkte baut.

Wettbewerb ist eine spätere Erfindung, in den berühmten Worten August Hayek's «ein Verfahren zur Entdeckung von Tatsachen, die ohne sein Bestehen entweder unbekannt bleiben oder doch zumindest nicht genutzt werden würden.» (Hayek 1968) Durch Wettbewerb ermittelt eine Gesellschaft, was sie produzieren will.

Heute würden wir sagen: Wettbewerb und Vertragsfreiheit korrelieren. Das ist die Lehrbuchweisheit.

Und TC? Wie verhält sich TC zu diesem Elementarprinzip freier Gesellschaften? Wieder fand ich die Idee von Dirk Kuhlmann hilfreich: Eine Plattform ist unvermeidlich. Aber wir kennen noch nicht ihr Ordnungsprinzip. Ein, wenn nicht das Ordnungsprinzip, für die Informationsgesellschaft.

Wir müssen wohl auf ein Wunder warten. Das kann dauern. Aber ohne Wettbewerb werden wir warten, bis wir schwarz sind.

Als Wissenschaftler könnte man jetzt jubeln: Endlich ist die Forschungslücke identifiziert. Man bräuchte nur einige Millionen Euro und fünf Jahre Zeit, um erste vorläufige Antworten zu formulieren.

Als Politiker wäre man sicher nicht amüsiert. Was soll man seinen Wählern in der Zwischenzeit erzählen?

Vielleicht gibt es eine dritte Strategie.

Die verlangt aber auch Mut.

Zunächst müssen wir Abschied von einer Gewissheit nehmen: Es gibt nicht so etwas wie eine Weltmoral, Weltgewalt. Wir haben auch nur «fälschlich» angenommen, dass eine Weltrechtsordnung uns Antworten auf das Ordnungsproblem gibt. Es gibt kein Prinzip für diese und andere Plattformen.

Wir müssen auch verstehen, dass nicht Staaten, sondern neuartige Akteure wie das TC-Konsortium auf den Plan getreten sind. Sie tun etwas, was Lawrence Lessig aus Stanford «Code-Regulierung» nennt. Ordnung wird nicht durch Recht, sondern durch Code hergestellt. (Lessig 1999)

Keine Bange: Ich weiß, was sich gehört. Ich habe Alfred's erhobenen Zeigefinger nicht vergessen. Ich denke pausenlos an ihren knurrenden Magen und Ihren verschämten Blick auf die Uhr.

Abschiednehmen genügt nicht. Das entscheidende Moment dieser Strategie ist es wohl, sich überhaupt auf das Verfahren der Entdeckung einzulassen. Die Gedanken vielleicht noch einmal umzusortieren.

Hier hat Kunst ihre aus meiner Sicht wichtigste Funktion.

Sie haben das Glück, in einem der wichtigsten Museen für moderne Kunst in der Welt speisen zu dürfen.

Da «gibt» es in diesem Flügel da einen Beys, der mal gesagt hat: Alle sind wir Künstler. Muss man nicht teilen. Meine Frau jedenfalls ist entsetzt.

Hier unten, im Herz des Bahnhofs wird es spannend. Hier ist Andy Warhol ausgestellt. Den halte ich für den wichtigsten Künstler des ausgehenden 20. Jahrhunderts. Ein Bild besonders hat mich fasziniert. Ich habe den Hamburger Bahnhof schon besucht, nur um mir dieses eine Bild noch einmal anzugucken.

*Do it yourself (Seascape) von 1962*



Sein wir wie Kinder.

Du kannst die Welt gestalten. Du hast alle Bausteine, die Du brauchst.

Alles passt zusammen. Eine perfekte Welt.

Modelliere die Welt. Sei ihr Baumeister.

Ein perfekter informatischer Traum.

Schauen Sie sich jetzt einmal die Wolken an.

Wolken bewegen sich. Sind weiß. Aber nicht nur. Wo kommt das Dunkle her? Sonne, aufsteigende Feuchtigkeit und Thermik. Sei die Sonne.

Aber Du bist ja nur ein Mensch.

Schauen Sie sich jetzt die Seemöwen an.

Die sind Lebewesen, die fliegen. Und sie sind weiß.  
Das Weiß hat keine Ziffern. Ist gesetzt, sozusagen die Default-Einstellung.

Denken Sie sich jetzt das Weiß weg.

Da bleibt nichts mehr.

Oder etwa das Schwarz?

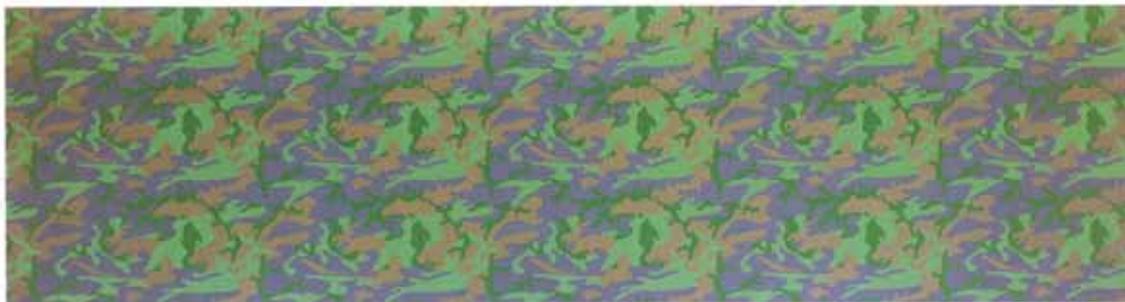
Auch das ist gesetzt, hat keine Ziffer. Leere auf dem Papier. Aber auch im Kopf?

Andy Warhol als Meister der Gestaltung von Oberflächen: Je mehr Du schaust, umso unklarer wird alles.

Manchmal gibt es im Leben seltsame Zufälle: Am Montag letzter Woche habe ich an meinem Schreibtisch über diesem Vortrag gebrütet.

Vielleicht kennen Sie das auch bei sich: Wenn mir nichts einfällt, erfinde ich dauernd wichtige Ablenkungen. Ich wasche mir zum Beispiel dauernd die Hände. Ich beschloss, mich mit der Lektüre der F.A.Z. abzulenken. Eigentlich habe ich nur lustlos rumgeblättert, um die Zeit tot zu schlagen. Auf einmal fällt mein Blick auf ein Bildmotiv im Hamburger Bahnhof:

*Andy Warhol, Camouflage von 1986*



Camouflage: Tarnen, täuschen, Tarnanzug.  
Soldaten oder nur so ein Spiel? Oder die neueste Mode?  
Wer oder was wird verborgen?  
Wer soll getäuscht werden?

Der junge und der alte Warhol sind sich treu geblieben: Das Spiel mit der Oberfläche als Thema. Der junge Warhol gibt uns eine Fluchtmöglichkeit aus dem Bild. Der alte wohl nicht. «Warhol malt nicht die Sache selbst, sondern das Gefühl, das sie auslöst.» (de Salvo 2001, S. 49)

Was mich nun besonders überrascht und gefreut hat, war die offensichtliche Überlegung des Bildredakteurs: Da gab es einen ganzseitigen Artikel des Soziologen Otto Hondrich über Weltgewalt und Weltrechtsordnung, über die moralischen Prinzipien gesellschaftlicher Organisation, über den Abschied von alten Glaubenssätzen.

Wie nimmt man so einer intellektuellen und emotionalen Herausforderung die Wucht? Indem man die bleischweren Gedanken Hondrichs mit der unpersönlichen Bildstrategie Warhols konfrontiert. Wenn die Leserin keine Lust mehr hat, könnte sie sich das Bild ansehen.

Mit diesem Befund sollten wir Normalmenschen für heute zufrieden sein: Alles sehr schwierig. Vorsicht ist angesagt.

Bilder sagen mehr als tausend Worte, sagt das Sprichwort – allerdings nicht immer.

Sollten unter uns Politiker weilen, möchte ich sie nicht so einfach in die Welt der Oberflächen entlassen. Von ihnen verlange ich, dass Sie den Artikel von Hondrich tatsächlich lesen. Sie müssten nur ein wenig Phantasie haben. Dann würden Sie entdecken, dass Hondrich ein strategisches Movens entfaltet, das zum Kern meiner dritten Strategie werden könnte. Gesellschaften figurieren sich von alleine nach Prinzipien, die Ordnung schaffen. Diese Sehnsucht nach Ordnung kann und muss man beflügeln, indem man dem Entdeckungsverfahren Wettbewerb Raum lässt. Ich kann mich täuschen: Einige der Prinzipien Hondrich's klingen sehr stark nach dem Open Source Prinzip – Prinzip, nicht Software.

Vielleicht ist mir so eine perfide Strategie gelungen:

Die einen werden jetzt schleunigst den Raum verlassen, um unverzüglich die F.A. Z. zu lesen.

Die anderen stehen schon in den Startlöchern, um endlich die Originale von Andy Warhol anzuschauen.

Bleibt ein verschwindener Rest.

Mit dem werde ich jetzt das Dinner einnehmen – mit viel Platz und noch mehr Speise.

