Die Datenschleuder

DM 5,00

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

Nummer 26/27 I Nov. 1988

Delx (entartet)

Doppelnummer

DES
Verschlüsselung

CoCom

BTX

Banken greifen
Meldedaten

Computer:
Soziologennutzug
im Alltag

Wie
Chaos
entsteht

**Chaos
Communication
Congress '88**

Ist Freiheit vektorisierbar?

– Die Heidelberger Computerposse –

Ende 1987 beschloß das Universitäts-Rechenzentrum (URZ) der Universität Heidelberg – im Alleingang, wie sich später herausstellte, d.h. ohne Absprache mit der Universitätsleitung – die Aufnahme eines neues Paragraphen in den jährlich neu zu stellenden BenutzerInnen-Antrag (siehe unten). In ihm wurde der *Ausschluß von Studierenden* aus dem Ostblock für den Fall festgeschrieben, daß am URZ eine sogenannte Vector-Facility (VF) installiert wird. Dieser Hardwarezusatz, der die URZ-eigene IBM 3090-180 für bestimmte mathematische Operationen (parallelisierbare Vektor- und Matrixrechnungen) bis zu einem *Faktor vier beschleunigt*, fällt unter die Bestimmungen der CoCom-Liste. Das Coordinating Commitee for East-West Trade Policy – kurz CoCom – überwacht seit den Zeiten des Kalten Krieges den Know-How–Transfer westlicher „Hoch"technologie in den Ostblock. Daß sich die Universität hierzulande in blindem Gehorsam zum Vollzug unzeitgemäßer NATO-Interessen bereit erklärt hat, ist nicht nur enttäuschend, sondern im Sinne der freiheitlich-demokratischen Grundordnung auch eine schlimme Fehlentscheidung.

Das Treffen von Fehlentscheidungen ist etwas Verzeihliches; Menschen müssen fehlbar sein dürfen. Der Unterschied zwischen einer Demokratie und einer Diktatur liegt aber in ihrer Fähigkeit, Kritik an Fehlentscheidungen nicht zu eliminieren, sondern diese Kritik ernstzunehmen und wenn nötig, Entscheidungen auf Grund berechtigter Kritik zu korrigieren. Kritikfähigkeit ist ein Kind der Freiheit; deshalb sind Demokratie und Freiheit synonym. *Aber Freiheit, sagt Rosa Luxemburg, ist immer auch die Freiheit der Andersdenkenden.* Der Ausschluß von Studierenden aus dem Ostblock auf Grund eines ideologischen Dogmas ist ein Schlag in das Gesicht der Demokratie. Eine Universität, die für sich in Anspruch nimmt, eine demokratische Institution zu sein und aus den Fehlern der Vergangenheit gelernt zu haben, sollte Angesichts solcher Entscheidungen Scham empfinden. Die Vertreibung linker, jüdischer und liberaler Professoren und Studierender von den Universitäten im Dritten Reich hat nicht nur dem Ansehen, sondern auch der Wissenschaft einen auch heute nicht überwindbaren Schaden zugefügt.

Daß die *Entscheidung* von der Universität jedoch nicht zurückgenommen, sondern nur durch haushaltspolitische Argumente *aufgeschoben* worden ist, deutet darauf hin, daß die Universität infolge der Ablehnung ihrer Entscheidung in den Medien mehr ihr öffentliches Ansehen retten als ihr demokratisches Grundverständnis unter Beweis stellen will, auch wenn sie es im Nachhinein so darstellt. Daher müssen die weiteren Entscheidungen der Universitätsleitung und des URZ nicht nur in Bezug auf den Rechnerausbau solange genaustens beobachtet werden, wie die Universität ihre Klugheit nicht demonstriert – denn George Bernhard Shaw sagt: **"Der Unterschied zwischen dummen und klugen Menschen ist sehr gering. Beide machen Fehler. Aber dumme Menschen machen den gleichen Fehler immer wieder; kluge Menschen machen immer neue Fehler."**

(Bernd Fix, stud. Vertreter im EDV-Ausschuß der Universität Heidelberg)

Sofern 1988 an der Anlage IBM3090 eine Vector-Facility installiert wird, dürfen Angehörige der Länder Afghanistan, Albanien, Bulgarien, CSSR, DDR, Kambodscha, Kuba, Laos, Libyen, Mongolei, Namibia, Nordkorea, Polen, Rep. Südafrika, Rumänien, UdSSR, Ungarn, Vietnam, VR China oder Organisationen dieser Länder aufgrund von Bestimmungen der Ausfuhrbehörde der USA nicht zur Nutzung der Anlage zugelassen werden. Ebenso dürfen Projektnummern nicht Angehörigen oder Organisationen dieser Länder zur Nutzung überlassen werden. Der Institutsleiter oder sein Beauftragter bestätigt durch seine Unterschrift, daß der Bearbeiter nicht zum oben genannten Personenkreis zählt. Der Bearbeiter erkennt durch seine Unterschrift diese Bestimmungen ausdrücklich an. Bei Nichtbeachtung oder Mißbrauch ist der betreffende Bearbeiter schadensersatzpflichtig.

Privater Nachrichtenschutz mit PC-DES

Grundsätzliches

Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich
(Artikel 10 Absatz 1 des Grundgesetzes)

Nach dem Grundgesetz steht also allen Menschen das Recht zu, ihre privaten Nachrichten vor dem Einblick Dritter zu schützen. Die Verwendung der Verschlüsselungsmethoden für die Nachrichtenübermittlung ist seit den 60er Jahren dank der technischen Entwicklung eine einfach zu handhabende Sache, die es allen Menschen erlaubt, ihre informationelle Selbstbestimmung selbst wahrzunehmen.

Darüber hinaus besteht ein allgemeiner Bedarf für die Verschlüsselung der Nachrichteninhalte. Verfahren hierfür sind bekannt. Da im ISDN auch die Sprache in digitaler Form vorliegt, bietet sich auch eine durchgehende Sprachverschlüsselung von Teilnehmer zu Teilnehmer an. Aufgrund von Bedarfsanalysen geht die Deutsche Bundespost davon aus, daß die Verfahren als öffentlicher Verschlüsselungsdienst im Sinne zusätzlicher Leistungsmerkmale des Fernmeldedienstes zu realisieren sind. Schon jetzt bestehende Möglichkeiten, private Verschlüsselungstechniken einzusetzen, bleiben davon unberührt.

(net special, Oktober 1985, Seite 104)

Die Bundespost erlaubt auch im ISDN die Verschlüsselung übermittelter Daten, wenn der dabei in Anspruch genommene Dienst nicht die Verschlüsselung der Texte verbietet (z.B. Telex-Dienst; nach §§ 5, 16, 17 TKO nur die Klartextweitergabe erlaubt). Die Datenfernübertragung zwischen Computern über den integrierten DATEX-P-Dienst erlaubt Verschlüsselung.

Die Strafprozeßordnung (§ 100 StPO) bestimmt, daß der Richter und, bei Gefahr im Verzuge, auch der Staatsanwalt die "Überwachung und die Aufnahme des Fernmeldeverkehrs auf ***Ton*** träger" anordnen können. "Auf Grund der Anordnung ***hat*** die Deutsche Bundespost dem Richter, dem Staatsanwalt und ihren im Polizeidienst tätigen Hilfsbeamten das Abhören des Fernsprechverkehrs und das Mitlesen des Fernschreibverkehrs ***zu ermöglichen***", § 100b (3) StPO.
Das Gesetz zu Art.10 Grundgesetz G 10 berechtigt unter bestimmten Voraussetzungen die Verfassungsschutzbehörden des Bundes und der Länder, das Amt für Sicherheit der Bundeswehr und den Bundesnachrichtendienst dazu, dem Brief-, Post- und Fernmeldegeheimnis unterliegende Sendungen zu öffnen und einzusehen, sowie den Fernschreibverkehr mitzulesen, den Fernmeldeverkehr abzuhören und auf ***Ton*** träger aufzunehmen, Art.1 § 1 (1) G 10.

(aus DuD-Fachbeiträge 6, Karl Rihaczek, Datenverschlüsselungen in Kommunikationssystemen – Möglichkeiten und Bedürfnisse – Vieweg 1984, Seite 249), Hervorhebungen da-red

„Sind Sie sicher, Miß Trebble, daß damit keinerlei militärische Zwecke verknüpft sind?"

Allgemeine Informationen zum DES

Der DES (Data Encryption Standard) ist ein Verschlüsselungsalgorithmus, der von IBM aus einem anderen Chiffrieralgorithmus, dem sogenannten LUCIFER - Algorithmus, entwickelt wurde. Dieser ebenfalls von IBM entwickelte Umsetzungsalgorithmus war als ein Block-Chiffre konzipiert worden und arbeitete mit einer Schlüssellänge von 128 Bit. Für den DES wurde die Länge des Schlüssels auf 56 Bit gekürzt, was einige Kritiker des DES-Algorithmus zu der Annahme gebracht hat, daß die NSA (National Security Agency als amerikanischer Nachrichten-und Geheimdienst) die Verkürzung des Schlüssels zu verantworten hat. Tatsache ist, daß die NSA an der Entwicklung und am Sicherheits-Check des Algorithmus regen Anteil genommen hat. Darauf wird nochmals im Abschnitt 3.4 näher eingegangen, wo Fragen und Überlegungen zur Sicherheit des DES besprochen werden.

Jetzt soll aber zuerst in einer kurzen Beschreibung die Art der Chiffrierung durch den DES dargestellt werden.

Die Verschlüsselung

Zuerst wird aus einem einzugebenden 64 Bit Schlüssel (8 Bytes) durch eine Auswahl von 56 Bit ein effektiver Schlüssel erzeugt. Die übrigen 8 Bit des Eingabeschlüssels dienen als Paritätsbits und sollen fehlerhafte Schlüssel erkennen helfen. Aus dem erzeugten 56 Bit Schlüssel werden in einer Prozedur die für den eigentlichen Krypto-Vorgang benötigten 16 Arbeitsschlüssel mit einer Länge von jeweils 48 Bit erzeugt. Diese Schlüssel heißen in der Reihenfolge ihrer Generierung K1 . . . K16. Der Quelltext, der verschlüsselt werden soll, wird in Blöcke von je 64 Bit zerlegt. Dieser 64 Bit Eingabeblock wird dann zuerst in einer Eingangspermutation IP vertauscht. Das Ergebnis dieser Prozedur durchläuft dann 16 mal eine Schleife, in der es mit dem jeweils nächsten Schlüssel Kn umgesetzt wird. Das vorläufige Endergebnis wird noch einmal mit der zu IP inversen Permutation umgeordnet und stellt danach den Zielcode der Chiffrierung dar: das Chiffrat.

Die Entschlüsselung

Die Entschlüsselung eines Programms ist mit der Verschlüsselung praktisch identisch; der einzige Unterschied ist die Reihenfolge der Schlüssel Kn bei der Chiffrierung. Während die Abfolge der Arbeitsschlüssel bei der Verschlüsselung K1, K2, . . . , K16 lautet, ist die Reihenfolge bei der Entschlüsselung die genau umgekehrte, also K16, K15, . . . , K1. Ansonsten wird der Algorithmus nicht modifiziert.

Die Betriebsarten des DES

Bei der Anwendung des DES werden vier unterschiedliche Betriebsarten eingesetzt, die entweder eine Blockchiffre oder eine kontinuierliche Chiffre ermöglichen. Die benutzten Betriebsarten sind:

Electronic Code Book Mode, ECB

In diesem Modus wird der Eingangstext in jeweils 64 Bit lange Blöcke zerlegt, die dann sequentiell umgesetzt werden. Für den Fall, daß der letzte Block weniger als 64 Bit enthält, wird er einfach aufgefüllt, zum Beispiel mit Nullen. Diese Betriebsart ist im Programm PC-DES implementiert.

Cipher Block Chaining Mode, CBC

Wie beim ECB wird der Quelltext in 64 Bit-Blöcke zerlegt. Falls der letzte Block kürzer ist als 64 Bit, so wird er entweder mit einer vorher definierten Bitsequenz aufgefüllt oder es wird für diesen letzten Block eine eigene Prozedur zwischen Empfänger und Sender vereinbart. Der generelle Ablauf des CBC-Modus ist folgender:

Zuerst wird zwischen Empfänger und Sender ein Initialisierungsvektor IV von 64 Bit Länge vereinbart. Der Sender verknüpft nun den zu sendenden Block exklusiv-Oder mit diesem Vektor IV. Das Ergebnis wird durch den DES-Algorithmus chiffriert. Der Output des DES wird für den Sender der nächste IV-Vektor. Der Empfänger dechiffriert den empfangenen Block mit dem DES - Algorithmus und verknüpft das Ergebnis mit seinem IV ebenfalls exklusiv Oder. Der ursprünglich empfangene Block wird zum nächsten IV des Empfängers. Die gesamte Prozedur wiederholt sich bis zum Ende des Quelltextes beim Sender.

Cipher FeedBack Mode, CFB

Die beiden vorherigen Verschlüsselungsmodi waren Block-Chiffren mit einer Länge von 64 Bit, die in einem Schritt umgesetzt wurden. Für manche Anwendungen kann es notwendig sein, einen Block geringerer Länge zu chiffrieren. Die Cipher FeedBack - Methode erlaubt die Umsetzung von Blöcken mit einer Länge von ein Bit bis 64 Bit in stufenloser Abfolge. Dazu arbeitet der DES sowohl auf Sender- als auch auf Empfängerseite im Verschlüsselungsmodus. Hier der schematische Ablauf des CFB-Modus; die Länge des umzusetzenden Blocks betrage k Bit.

Zu Beginn der Verschlüsselung wird der Vektor IV sender- und empfängerseitig mit dem gleichen Bitmuster geladen. Vom Output des DES werden jeweils die ersten k Bit benutzt, entsprechend der Länge des zu chiffrierenden Blocks. Diese k Bit werden dann Exklusiv-Oder mit dem Klartext-Block verknüpft und dem Empfangenden übermittelt. Die k Bit des DES - Outputs werden gleichzeitig noch von rechts nach links in den DES - Inputvektor IV geschoben und sind damit Teil des nächsten Inputs für den DES. Empfängerseitig werden k Bits empfangen. Diese k Bits werden zuerst von rechts nach links in den Inputvektor IV geschoben, der DES - Output berechnet und die ersten k Bit dieses Outputs werden daraufhin mit den empfangenen k Bits Exklusiv-Oder verknüpft und liefern den k Bit langen Klartext-Block.

Diese Betriebsart des DES ist natürlich nicht so effizient wie die Block-Modi, weil für jeden Block kürzerer Länge auch ein vollständiger Durchlauf durch des DES - Algorithmus nötig ist.

Wie auch die letzte Betriebsart hat der CFB-Modus Ähnlichkeit mit den sogenannten Running-Key-Cipher – Algorithmen, weil der Klartext zur Verschlüsselung mit einem "laufenden", d.h. kontinuierlichen Verschlüsselungstext logisch Exklusiv-Oder verknüpft wird.

Output FeedBack Modus, OFB

Auch in dieser Betriebsart wird ein kontinuierlicher Verschlüsselungstext mit einer variablen Länge k ($1 \leq k \leq 64$) erzeugt und mit dem Klartext-Block Exklusiv-Oder verknüpft. Im Gegensatz zum CFB-Modus werden allerdings die k Bit des DES-Outputs, die zur Verschlüsselung verwendet werden, von rechts nach links in den DES - Inputvektor IV geschoben und zwar sowohl sender- als auch empfängerseitig. Zur Synchronisation muß der IV zu Beginn der Übertragung mit dem gleichen Bit-Muster initialisiert werden. Auch hier ist die Effizienz natürlich geringer als in den Block-Modi.

Sicherheitsbetrachtungen zum DES

Seit der Veröffentlichung des DES und vor allem seit der Normierung zum US-Verschlüsselungsstandard gibt es einige Kritiker, die den DES für nicht so sicher halten, wie es in den Erklärungen von IBM u.a.m. dargestellt wird. Ihre Hauptkritikpunkte sind die folgenden drei Überlegungen.

(1) Die meisten Kritiker halten die Schlüssellänge von 56 Bit im effektiven Schlüssel für zu kurz und fordern die Erhöhung der Schlüssellänge um mindestens 72 Bit auf insgesamt 128 Bit, was auch dem ursprünglichen LUCIFER - Algorithmus entsprechen würde.

(2) Die Auswahlkriterien einzelner Bestandteile des DES - Algorithmus wurden bzw. durften von IBM nicht veröffentlicht werden. Dies betrifft vor allem die Auswahl der Substitutions-Boxen, von deren Ergebnisfunktion die Sicherheit ganz wesentlich abhängt.

(3) Ebenfalls nicht veröffentlicht wurden die von IBM und der NSA durchgeführten kryptoanalytischen Tests und Bewertungen der Sicherheit des DES.

Schlüssellänge

Zwei frühe Kritiker des DES, die Mathematiker Hellman und Diffie, schlugen eine Maschine vor, die in der Lage wäre, den DES "zu knacken". Das Prinzip der Maschine beruht auf einem sturen Austesten aller möglichen Schlüssel des DES und Kontrolle des damit erzielten Entschlüsselungsergebnisses. Für den Bau der Maschine müßte ein spezieller Mikroprozessor entwickelt werden, der mit einer hohen Geschwindigkeit die einzelnen Schlüssel testet. Zudem würden in einer solchen Maschine 10 hoch 6 solcher Chips parallel arbeiten, um eine kurze Suchzeit zu erreichen. Diese Maschine würde beim Stand heutiger Technik etwa 20 Millionen Dollar kosten, was für eine in ihren finanziellen Mitteln kaum beschränkte Behörde wie die NSA ein akzeptabler Preis wäre. Eine solche Maschine wäre in der Lage, alle 2 hoch 56 Schlüssel (7.2 x 10 hoch 16) in einem Tag ausprobieren, was eine mittlere Suchzeit von etwa 12 Stunden bedeutet. Würde die Maschine jeden Tag zwei Schlüssel ermitteln und das fünf Jahre lang, so würde bei Kostenumlegung jede Lösung etwa 5000 Dollar kosten. Nicht berücksichtigt bei dieser Überlegung ist sogar noch die Tatsache, daß sich das Preis/Leistungs-Verhältnis von Mikrochips alle vier Jahre verdoppelt und somit die Maschine immer billiger wird. Ihr Vorschlag besteht in einer Verlängerung der Schlüssellänge auf 128 Bit; eine Maschine zum Ermitteln einer solchen Schlüssellänge in auch einem Tag wäre technisch nicht realisierbar.

Wie schon oben erwähnt, beruhte die ursprüngliche Konzeption von IBM beim LUCIFER - Algorithmus auf 128 Bit; auf Ersuchen der NSA wurde diese Länge ohne Angabe von Gründen auf 56 Bit verkürzt, was selbstverständlich Anlaß für Zweifel sein kann. Der Informatiker Jacques Vallee drückt es so aus: "*Manche Wissenschaftler meinen, das Bureau of Standards hätte bewußt eine Schlüssellänge von solchem Umfang gewählt, daß Collegestudenten und die meisten Industriespione abgeschreckt werden, aber kurz genug, daß die Herren in Washington weiterhin anderer Leute Post lesen können.*"

Hellman schlägt vor, daß wenn schon die Schlüssellänge des DES nicht verändert und dennoch der Einsatz des DES gefordert wird, die Umsetzung eines Klartextes durch ein dreimaliges Durchlaufen des Algorithmus mit drei unterschiedlichen (!) Schlüsseln zu verwenden, was einer effektiven Gesamtschlüssellänge von 128 Bit entsprechen würde. Hardwaremässig könnte das durch ein Hintereinanderschalten (Pipelining) von drei DES-Prozessoren verwirklicht werden.

Entwicklungskriterien

Die Sicherheit des DES ist wesentlich von der Konzeption gewisser Teilkomponenten des DES abhängig. Auf Anweisung der NSA war

IBM nicht berechtigt, die Entscheidungsgrundlagen für die Auswahl bestimmter Teile des DES wie die Substitutionsboxen zu veröffentlichen, da sie der NSA als zu "sensitiv" erschienen. Kritiker vermuteten daher, daß in die Entwicklung des Algorithmus einige sogenannte "trap-doors", das sind Verkürzungen im Verschlüsselungsvorgang, eingeflossen sind, die es der NSA erleichtern würden, ein Chiffrat analytisch zu entschlüsseln.

Mittlerweile hat die NSA einige der Entwurfskriterien für die S-Boxen bekanntgegeben; trotzdem hält sich der Vorwurf einer nicht erklärten Einflußnahme des NSA auf die Entwicklung des Data Encryption Standards.

Sicherheitstests

Ebenfalls nicht veröffentlich wurden die kryptoanalytischen Untersuchungen, die IBM und die NSA bezüglich des DES durchgeführt haben. Die einzigen Verlautbarungen beschränkten sich auf die Feststellung, daß der DES in keinem dieser Tests die bekannten Schwächen anderer Verschlüsselungsalgorithmen gezeigt hat und daß daher die Sicherheit des DES bewiesen wäre.

Dieses Verhalten von Seiten der Entwickler veranlaßte zu Recht die Kritiker zu der Bemerkung, daß wenn der DES die Tests so gut bestanden hat, eine Veröffentlichung der Testergebnisse doch nur zu einer Anerkennung dieser Sicherheit führen könnte. Wenn diese Veröffentlichung jedoch unterbleiben würde, so müßte doch davon ausgegangen werden, daß sie die Sicherheit des DES eben nicht beweisen würden.

Alles in allem bleibt festzustellen, daß die Sicherheitsfrage für den DES noch nicht abschließend beantwortet werden kann. Bei besonderen Sicherheitsansprüchen kann durch dreimaligen Aufruf von PC-DES auch die von Hellman vorgeschlagene Erhöhung der effektiven Schlüssellange auf 128 Bit erreicht werden.

Ausblick

1988 hätte der DES von der NBS (National Bureau of Standards, nationale Standardisierungsbehörde der USA) erneut als Verschlüsselungsstandard benannt werden müssen. Dieses ist nicht geschehen. Der Grund: Die NSA will einen neuen und diesmal nur von ihr – und nicht in Verbindung mit externen Firmen wie IBM – entwickelten Verschlüsselungsalgorithmus zum Standard machen. Über diesen dürfe dann überhaupt nichts mehr bekannt werden, wie er intern arbeitet. Herstellerfirmen für die entsprechenden Verschlüsselungschips erhalten dann die Maske für den Chip und dürfen ihn nur noch produzieren. Um die Unsicherheit unter den DES-AnwenderInnen noch zu verstärken, wurde vor einem Jahr das Gerücht verbreitet, daß in den USA ein Freak ein Turbo-Pascal-Programm geschrieben hätte, das den DES in ein-einhalb-Stunden knacken könne. Leute vom ZfCh (Zentralstelle für Chiffrierung) meinen ebenfalls, daß es sich um ein Gerücht handelt. Es ist auch einleuchtend, bei der Einführung eines neuen Verschlüsselungsstandards dafür zu sorgen, daß der DES nicht mehr als Verschlüsselungsstandard anerkannt wird und die AnwenderInnen ihn für unsicher halten. Für mich ist das Vorhandensein des Gerüchtes Grund genug zu glauben, daß der DES sicher ist – zumindest so sicher, daß die NSA sich genötigt sieht, einen neuen (eigenen) Algorithmus vorzuschlagen.

DES-Verschlüsselungsprogramme waren bisher nicht einfach zu erhalten. VAX-Encryption z.B. wird nur an bestimmte Kunden zu horrenden Preisen vertrieben (siehe Datenschleuder 25, Seite 6f). IBM baut aus ihren Mainframe-Rechnern die dort serienmäßig vorhandene DES-Hardware-Verschlüsselungen aus, wenn sie z.B. in die BRD exportiert werden. Borland's Turbo-Key durfte nicht aus den USA exportiert werden, weil es ein DES-Verschlüsselungsprogramm enthielt. Aus diesen Gründen freut sich die Redaktion Datenschleuder, hier an dieser Stelle das in diesem unserem Lande entwickelte Programm **PC-DES** vorstellen zu können. Seit gut einem Jahr läuft eine Implementierung für IBM PCs und Kompatible mit einem optimierten Algorithmus, der auf einem 4.77 Mhz PC mit V20-CPU max. 135 Zeichen pro Sekunde umsetzen kann. Seit einem halben Jahr existiert auch eine Implementierung für IBM-Mainframes und Kompatible, **DES/370 (dieses Programm wurde im übrigen vollständig auf einem IBM–kompatiblen PC mit einem /370 – Crossassembler und Crossexecuter entwickelt. S/370? PC-SIG 402!)**. Durch weiteres Übertragen des Programmes auf andere Rechner lassen sich auch verschlüsselte Nachrichten austauschen. Wenn sich ProgrammiererInnen für die Rechner DEC/VAX, Atari, Commodore 64, Amiga, CP/M 80 usw. bereitfänden, den Algorithmus zu implementieren – erste Zusagen für Umsetzungen liegen schon vor –, wäre eine breite Basis für diesen Austausch geschaffen. Über dsred Rhein–Neckar, (Mitteilungsbox PF 104027, 6900 Heidelberg, dsred @ RNIHD .UUCP oder RNI–Mailbox (06203 / 45496): dsred), wird die Umsetzung des Programms für DEC/VAX und andere koordiniert. — © bf

BTX - Das Unsicherheitssystem

Manchmal sieht man den Wald vor lauter Bäumen nicht. Diese Binsenweisheit trifft auch mal wieder auf folgende Geschichte zu. Im Schwabenland kamen paar gecke Schwaben irgendwann mal auf die Idee, daß man sich mal BTX ansehen sollte. Sie zogen also aus, ein BTX-Terminal zu suchen. Jenes fanden sie dann auch. Dort nahm man die Gelegenheit wahr, sich die Hardwarekennung des Postmodems zu beschaffen. Dies geschah so:

Man nehme ein
Diktiergerät.
Ein paar Leitungen.
Ein paar Stecker.

Dann sieht man sich ein bissele um, und sieht:
NIX.

Also nix wie angeschlossen. Dies geht bei DBT03's meistens und manchmal auch bei öffentlich-rechtlichen BTX-Terminals.

Dann tippt man auf die allzeit beliebte Taste: VERBINDUNG AUFBAUEN. Es pfeift durch die Gegend. Der BTX-PAD pfeift zurück. Und dann gibt es noch ein Repfiff vom Modem. Das war's!!!

Die Schwaben gingen nach Haus mit dem festen Glauben, den Code entschlüsseln zu können.

Wollen wir es mal vorweg nehmen. Sie schafften es nicht. Der Grund: Es gab keine Codierung.

Angeschlossen an den heimischen Atari ST samt Terminal-Programm mit den BTX-Parametern 8N1 (BTX-Parameter) bekam man den berühmten Zeichensalat ohne Sinn und Verstand. Man denkt sich also. Die Post ist ja schlau. Die Hardwarekennung und das Paßwort (welches auch öffentliche BTX-Geräte besitzen) wird codiert rausgesendet. Ein besonders schlauer Schwab' meinte dann: 'Parameter ändern'. Man probierte und probierte und bei 7 Stopbits , Gerade Parity und 1 Stopbit bekam man sinnvollen Zeichensalat. Eine Nummer sowie ein Mädchennamen. Aber was nützt das...ist ja nun mal eine Hardwarekennung. Dann denkt man sich, die Hardware kann man sicher nachmachen. Also wird auf den Atari ST ein Assemblerprogramm programmiert, welches mit dem ST-Programm 'BTX-Term' zusammenarbeitet. Die ersten Versuche schlugen fehl. Der BTX-Pad legte auf, bevor die Nummer gesendet wurde. Nach einer Weile kam man dahinter, daß der BTX-Pad die Verbindungsaufnahme mit dem Senden einer logischen Null quittiert und dann genau 1,7 Sekunden auf die Hardwarekennung wartet. Dann begann etwas, was Programmierer hassen. Das Programm mußte optimiert werden.

Es wird wohl sicher Jubel ausgebrochen sein, als irgendwann mal der BTX-Pad die Hardwarekennung bestätigte und nach dem Paßwort fragte. Man gab dies ein und war in dem Blödeltextsystem der Post drin. Man rief Seiten auf, trieb sich in Eden rum, und schickte Mails durch die Gegend. Die Kosten trug der Besitzer des Modems (eine Firma).

Das war aber noch nicht alles. Irgendwann kam man auf den Gedanken, mit ein und derselben Hardwarekennung zugleich den BTX-Pad anzuwählen. Praktisch ist das natürlich ein Unding, da ja jede Hardwarekennung nur einmal vorkommen darf, aber die Post hat ja ein hervorragendes Mutilportsystem. Es funktionierte!

Zu diesem Zeitpunkt bekam der Autor von der Sache zu hören. Es interessierte ihn so, daß er um nähere Auskünfte bat. Mit einen Haufen mündlichen Informationen, machte er sich auf der CeBit'88 auf den Weg zum Poststand, an dem man sich mit BTX beschäftigte. Begleitet von zwei Freunden kam er dort in einem ziemlichen Getümmel an. Wir wandten uns an eine nette Dame und fragten nach jemanden der für BTX zuständig ist. Nach nur 5 Minuten meinte man zu uns: 'Das ist ihr Mann' und begleitete uns zu einem Tisch samt BTX-Terminal.

Meine Wenigkeit meinte dann, Guten Tag (man ist ja gut erzogen) und stellte mich als Mensch des CCC vor. Der Effekt des Postlers war sehenswert. Erst kam ein kurzer Nevernzusammenbruch mit der Bemerkung: 'Unsere persönlichen Freunde', dann ein Schrei über den halbe Poststand: 'Hans....Chaos Computer Club....HILFE !'

Nach dem Start fragte ich ihn mal über das BTX-System aus. Wie wird die Hardwarekennung gesendet, Schutz und so weiter. Ich erzählte in theoretischer Form über die Möglichkeiten des BTX-Hackens. Um uns sammelten sich Besucher und Postler. Inzwischen hatte ich den Postler schonend darauf vorbereitet, daß

die Theorie nicht nur Theorie ist. Es meinte dazu nur: 'Kein System ist 100%ig sicher!'. Das wollte er mir aber leider nicht schriftlich geben. Ein anderes Postler versuchte mit (guten) Argumenten unsere Theorie zu zerstören. Er kam mit zeitkritischen Kennungen, ist rechtlich strafbar, usw. Das letzte Argument gefiel mir am besten: 'Wir zwingen ja niemanden BTX, zu machen !'

Plötzlich wurde die Diskussion seitens der Postler abgebrochen. Erst fragte ich mich warum, dann sah ich mich um. Es hatten sich etwa 30 Leute angesammelt, die zuhörten.

Dann kam eine Weile nichts. Erst im Juli kam ich zum Treffen nach Schwaben und bekam dort die Software und die Tips zur Hardware in die Hand gedrückt.

Man erzählte mir was man so alles gemacht hat. Inzwischen hatte die Firma gemerkt, daß etwas nicht stimmt und hatte das Paßwort geändert. Aber nicht nur das. Diese Firma hat auch neue BTX-Plätze (Multitel). Mit denen kann man das Spielchen mit dem Diktiergerät nicht machen.

Mit der Software besuchte ich einen Freund in der Schweiz. Genauer in Zürich. Dort hat man ein BTX-ähnliches System namens Videotex. Die von der Schweizer Post (PTT) benutzte Software scheint dieselbe zu sein, wie die des BTX-Systems. In der Schweiz ist es einfacher die Hardwarekennung rauszubekommen, als in der BRD. Dort braucht man nur das Postmodem aufzuschrauben. Auf dem PROM ist ein Aufkleber mit der Hardwarekennung. Das Programm ausprobiert und gestartet und schon war man in Videotex. Das nennt man dann internationale Kompatibilität.

Das Assemberrprogramm selber ist inzwischen in Hamburg weiter optimiert worden. Durch reinen Zufall ist es auf der Druckerplatte gelandet:

```
/* HK-Emulator (c) beim Programmierer */

timera      EQU     $0134
scradr      EQU     $044E
dumpflag    EQU     $04EE
dumpvek     EQU     $0502

            MOVE.L  4(sp),A5
            LEA     own-stack(pc),sp
            MOVE.L  #own-stack,D0
            SUB.L   A5,D0
            MOVE.L  D0,-(sp)
            MOVE.L  A5,-(sp)
            PEA     $4A0000
            TRAP    #1
            LEA     12(sp),sp
            DC.W    $A000
            DC.W    $A00A

            PEA     main-txt(pc)
            MOVE.W  #9,-(sp)
            TRAP    #1
            ADDQ.L  #6,sp

            LEA     insert-str(PC),A3
            MOVEQ   #11,D2
L0004:      MOVE.W  #7,-(sp)
            TRAP    #1
            ADDQ.L  #2,sp
            MOVE.B  D0,(A3)+
            PEA     dummy-char(PC)
            MOVE.W  #9,-(sp)
            TRAP    #1
            ADDQ.L  #6,sp
            DBRA    D2,L0004

            DC.W    $A000
            DC.W    $A009

            CLR.L   -(sp)
            MOVE.W  #$20,-(sp)
            TRAP    #1
            ADDQ.L  #6,sp

            MOVE.L  #own-dump,dumpvek

            PEA     null(PC)
            PEA     null(PC)
            PEA     fname(PC)
            PEA     $4B0000
            TRAP    #1
            LEA     16(SP),SP

            CLR.W   -(sp)
            TRAP    #1

;*****************************************
;* Eigene "Hardcopy"-Routine
;*****************************************
;
own-dump:   MOVEM.L A0-A1/D0-D1,-(sp)
```

```
        MOVE      #$2700,SR
        MOVE.L    timera,old–timera
        MOVE.L    #own–timera,timera
        MOVE.L    scradr,A0
        LEA       78(A0),A0
        MOVEQ     #7,D0
L0006:  NOT.B     (A0)
        LEA       80(A0),A0
        DBRA      D0,L0006
        LEA       $FFFFFA01.w,A0
        BSET      #5,6(A0)
        BSET      #5,18(A0)
        BCLR      #5,14(A0)
        BCLR      #0,42(A0)
        BCLR      #0,44(A0)
        ANDI.B    #-$10,28(A0)
        MOVE.B    #$10,36(A0)
        BSET      #0,28(A0)
        MOVE.B    #-$52,40(A0)
        BSET      #0,42(A0)
L0007:  BTST      #7,42(A0)
        BEQ.S     L0007
        MOVE.L    scradr,A0
        ADDQ.L    #1,A0
        MOVEQ     #7,D0
L0008:  NOT.B     (A0)
        LEA       80(A0),A0
        DBRA      D0,L0008
        LEA       $FFFFFA01.w,a0
        MOVE.B    46(A0),D0
        CLR.W     D1
        MOVE.W    D0,D1
        CMP.B     #0,D1
        BNE.S     L0007
        MOVE.L    scradr,A0
        LEA       40(A0),A0
        MOVEQ     #7,D0
L0009:  NOT.B     (A0)
        LEA       80(A0),A0
        DBRA      D0,L0009
        LEA       $FFFFFA01.w,a0
        CLR.B     24(A0)
        MOVE.B    #-$5C,30(A0)
        MOVE.B    #7,24(A0)
        LEA       insert–str(PC),A1
        CLR.W     count
        CLR.W     L0015
        MOVE.B    #1,D0
        ANDI.W    #$2500,SR
L000A:  TST.B     D0
        BNE.S     L000A
        ORI.W     #$2700,SR
        MOVE.L    scradr,A0
        LEA       40(A0),A0
        MOVEQ     #7,D0
L000B:  NOT.B(A0)
        LEA       80(A0),A0
        DBRA      D0,L000B
        LEA       $FFFFFA01.w,a0
        MOVE.L    old–timera,timera
        BCLR      #0,42(A0)
        BCLR      #0,44(A0)
        MOVE.B    #$10,36(A0)
        MOVE.B    #-$76,40(A0)
        CLR.B     24(A0)
        MOVE.B    #7,24(A0)
        MOVE.B    #-$5C,30(A0)
        BSET      #0,42(A0)
        BSET      #0,44(A0)
        MOVEM.L   (sp)+,A0-A1/D0-D1
        MOVE.W    #-1,dumpflag
        ANDI.W    #-$C01,SR
        RTS

;*****************************
;* Eigene Timer-A-Routine *
;*****************************

own–timera: TST.W     count
        BNE       L000E
        CLR.W     D0
        MOVE.B    (A1)+,D0
        BEQ.S     L000D
        LSL.W     #1,D0
        ANDI.W    #$1FE,D0
        ORI.W     #$E00,D0
        MOVE.W    D0,L0017
        MOVE.W    #$A,count
        CLR.W     L0015
        MOVEQ     #1,D0
L000D:  BCLR      #5,$FFFFFA0F.w
        RTE
L000E:  LEA       $FFFF8800.w,A0
        MOVE.B    #14,(A0)
        MOVE.B    (A0),D0
        SUBQ.W    #1,count
        ROXR      L0017
        BCS.S     L000F
        ANDI.B    #-$11,D0
        BRA.S     L0010
L000F:  ORI.B     #$10,D0
        ADDQ.W    #1,L0015
L0010:  CMPI.W    #1,count
        BNE       L0011
        ORI.B     #$10,D0
        BTST      #0,L0016
        BNE.S     L0011
        ANDI.B    #-$11,D0
L0011:  MOVE.B    D0,2(A0)
        LEA       $FFFFFA01.w,A0
        MOVEQ     #1,D0
        BCLR      #5,$FFFFFA0F.w
        RTE

count:      DC.W    0
dummy–char: DC.B    '-',0
main–txt:   DC.B    27,'E',10,10,10,10
        DC.B    9,'BTX-HK-Emula'
        DC.B    'tor V676784'
        DC.B    13,10,10,10
```

```
                DC.B        'Deine Hardware-
kennung: ',0
L0015:          DC.B        0
L0016:          DC.B        0
L0017:          DC.W        0
old-timera:     DC.L        0
insert-str:     DC.B        '000000000000'
                EVEN
null:           DC.W        0
fname:          DC.B        'BTX-TERM.PRG',0
                bss
                ds.l        256
own-stack:      ds.l        0
```

Das Programm ist leicht zu benutzen. Man lädt den HK-Emulator und wird nach einer zwölfstelligen Hardwarekennung gefragt. Diese tippt man ein. Dann wird das Programm 'BTX-Term' (kann man kaufen) nachgeladen. Man schnappt sich sein Koppler und wählt den BTX-Pad für Hardwarekennungen an und wartet auf den Carrier. Wenn der da ist, legt man den Hörer auf den Koppler und drückt (SCHNELL !!!) Alternate Help auf dem Atari ST. Das Programm simuliert jetzt ein DBT03 für BTX. Wenn die Verbindung hergestellt werden konnte, wird BTX-Term gestartet, man bekommt das Einschaltbild der Bundespost und darf das Paßwort eingeben. Das war's. Die Parameter für den Koppler sind 8N1.

Das ganze klappt natürlich auch bei öffentlichen BTX-Terminals. Wenn man mal ein Terminal findet, was ein bissele Abseits steht und schlecht besucht ist, man siehe sich da mal auf Bahnhöfen, IHK und Flughäfen um, kann man die Hardwarekennung des Terminals (geht nur vereinzelt) samt Paßwort rausfinden. (Anm. dsred: 1. verboten, 2.geschickt getarnte Videoüberwachung, 3. neue Modellreihe) Gerüchten zufolge soll das Paßwort immer BTX oder POST sein. Eine ganz interessante Variante ist dann noch, daß man ja keine gebührenpflichtige Seiten von öffentlichen BTX-Terminals aufrufen kann. Das liegt daran, daß (nicht wie man denken könnte beim PAD) im PROM des Terminal verankert ist, die Bestätigung von solchen Seiten (das ist die 19 für JA) abzufangen. Das heißt aber auch, daß wenn man von zuhaus BTX macht, die Sperre fehlt. Das heißt: BTX umsonst.

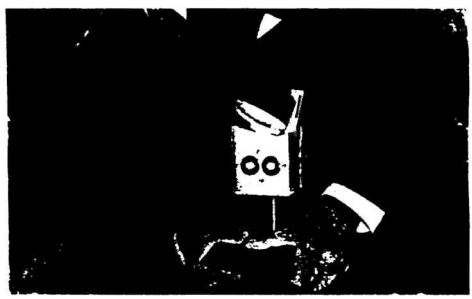
Und alles nur, weil es die Möglichkeit des Abhörens von HK und Paßwort gibt, was durch codieren der rausgesendeten Daten möglich wäre. Für den Otto-Normalverbraucher zuhaus besteht kaum Gefahr. Außerdem ist er durch TAN's und PIN's bezüglich Buchungen auf Bankkonten gut geschützt. Diejenigen, die Probleme damit bekommen, sind Firmen oder Banken, die in ihren Filialen BTX-Modems rumliegen haben. Betrüger gibt es überall.

Allerdings wollen wir mal nicht so sein....wir geben der Post folgenden Tip:

Fangt die 19 im Pad ab und nicht im Terminal und gebt Nummern frei, daß jeder DFÜ'ler der will legal von zuhaus BTX machen kann. Ortstarif aber bitte. Das aber bitte umsonst, dafür eben nur begrenzt nutzbar. Das ist doch eine Werbung. . .

Terra 151133@DOLUNI1.Bitnet

„Technik ist ein Lustobjekt des Mannes“



Schreine im Weltall

Die geostationäre Weltraumkolonie eines Rupert Mördok wird in Bälde über drei PAL-Kanäle das zur Erde senden, was der Medienzar zur Realität machen will. Die Firma Amstrad plant die dazugehörige Empfangsanlage zur Uni(n)formiertheit für nur noch 199 engl. £ vermarkten.

Der angekündigte Antennengewinn von 36 dB erstaunte die Experten und sei „nur mit sophistischer Technik realisierbar“. Die Sophisten galten im antiken Griechenland als ideologische Allesverkäufer. Die Firma Amstrad hat schon mit ihrem Schneider-Computer bewiesen, daß man durch Einsparung am wichtigsten Bit eine Menge Kohle machen kann.

Satellitensendestrecken sind Autobahnen in die Köpfe der Menschen – alles rauscht vorbei. . .

SOZIOLOGEN, ALLTAG & COMPUTER
Was haben Kuenstler damit zu tun?

Unglaublich. Ein Experiment.

Zur Vorgeschichte: Eine Handvoll Soziologie-Wissenschaftler stoßen im Rahmen ihres Forschungsprojektes "Computernutzung im Alltag" auf computernde Künstler. Sie geben den Künstlern die Möglichkeit, auf einem Kongress über dieses Thema, sich mit ihrer Arbeit zu präsentieren. Wovon auch die Künstler ausgiebig Gebrauch machen. Weitaus weniger interessierten sich die eingeladenen Soziologen für die Arbeit der Künstler. Ganz im Gegensatz zu den Künstlern. Sie hörten zwei Tage lang sehr intensiv den Ausführungen der Referenten zu. Ihr Tagungsbericht "KUNST UND COMPUTER" ist ganz im Sinne einer 'wissenschaftlichen Pantomime'gehalten:

"Da haben wir also Eure Methode zu arbeiten einmal übernommen und damit herumexperimentiert. Rein **künstlerisch. Versteht sich.** vergl.Zipper/Rammel, Band VI Seite 12 links oben, 3.Wort

Wir begannen mit einer Themensammlung. Wir gingen von den - uns durch Vorstudien bekannten - Eigenheiten aus. Dabei stützten wir uns im Besonderen auf eine Veranstaltung im ZIF und der 2-tägigen "teilnehmenden Beobachtung" von Soziologen oder Soziologie-Wissenschaftlern. Daher resultieren die im folgenden immer wieder auftauchenden Begriffe wie "Programm", "Tellerrand" oder gar der Begriff "87,5%", auf den wir weiter unten noch eingehen werden.

Wir fertigten also eine Begriffssammlung an und standen nun vor dem Problem, diese Sammlung auszufeilen, zu ergänzen und - wegen des doch gewaltigen Umfangs von Daten - Streichungen vorzunehmen. Zu diesem Zwecke begaben wir uns in ein einschlägig vorbelastetes Lokal (vier Tage zuvor hatte dort eine illegale **Bit-Napping Party**1 stattgefunden). Das Lokal zeichnet sich im übrigen durch ein sehr heterogenes Publikum aus. Weiterhin war uns gerade diese Lokalität von Frau Professor

1 spezielle Bielefelder Variante einer sozialen Einrichtung zum kostenlosen Austausch von Informationen.

Anm.: ZIF = Zentrum für interdisziplinare Forschung, Bielefeld

Luttmann sehr ans Herz gelegt worden. [2] Wir wählten nach repräsentativen Zufallssystemen einen Tisch aus. Wir setzten uns an genau jenen Tisch, an dem exact noch zwei Stühle frei waren. Nach genau 48 Minuten, als wir eine Bemerkung darüber machten, daß der Kellner uns permanent übersah, kamen wir in Kontakt mit jungen Menschen an unserem Tisch. Sie waren drei Jahre älter als wir und warteten ebenfalls auf den Kellner. Dies war eine hervorragende Gelegenheit, eine empirische Studie zu beginnen. Leider mußten die Jungs flippern und wir waren gezwungen, uns an ein junges Paar am Nachbartisch zu wenden, was eine Welle der Verzögerung auslöste und immense Kosten verursachte. Wir geben das Gespräch in Auszügen wieder:

sie: Heiß heute wah?

wir: äh ja. hähä. Dürfen wir Euch einmal etwas persönliches fragen?

sie: ?? äh, klar.

wir: Schafft es Euch Befriedigung, hier zu sitzen und zu dürsten?

sie: ??häh??was? äh nee. Natürlich nicht. Wolltér ein'n ausgeben?

wir: Nein, wir sind Wissenschaftler und siehe Dr.Fromm, "Sizilianische Eröffnung" und sind nicht zum Vergnügen hier...

...

Ok, wir machen im Manuskript weiter. Ergiebig wurde das Gespräch in dem Moment, als die Angesprochenen die Initiative ergriffen. Um sie nicht zu verscheuchen, haben wir unsere Arbeit als Spiel getarnt. Wir haben ihnen unsere erarbeiteten Begriffe vorgelegt und ihnen erklärt, daß sie nun weitere Begriffe hinzufügen, wegstreichen oder ändern können.

Vorgegeben waren die folgenden Begriffe:

Essen, Kaffee, Kantine, Auftrag, Gesundheit, Arbeit, Broterwerb, Dinge, Sachen, Eigenarten, Fotokopie, Befähigung, Alt, 87,5%=24, Ernst I, Ernst II, Tellerrand, Mädchen, Möglichkeit, Neugier, Funktion, Objekt, Gnade

Im Verlauf unsrerer Feldstudie wurden die folgenden Begriffe hinzugefügt:

[2] Frau Prof.Luttmann ist Autorin der sich selbst fortschreibenden Bücherreihe: "Wie mann aus fünfen eines macht"

Bratwurst, Schlaf, Zeit, Bier, Programm, Hampelmänner, kompliziert, Wissenschaft, positiv, zerstören, Schlonz, Musik, Datentankstelle, Denken, aussaugen, Gerätekrake, Trotzreaktion, Silikonkasten, Jungs, Popel, LebensWert, Lachen, Droge, Luis Trenker[3]

gestrichen wurde:

Wissenschaft, positiv, zerstören (zerstören kam vom männlichen Teil unseres Gegenübers. Als wir ihn auf das kindliche seines Tuns aufmerksam machten, strich er sofort das Wort "zerstören" und schrieb stattdessen das Wort "Trotzreaktion", das er nach einer kurzen Weile mit dem Wort "positiv" ergänzte. "positiv" wurde von seiner Freundin gestrichen.

Broterwerb, Kantine, Gnade (es ist eine Gnade, arbeiten zu können),

Objekt, Gesundheit, Bier (bei diesem Wort waren sich alle einig, daß dieses Wort mit der Nähe zur allgemeinen realen Situation - Kneipe - zu tun hatte; siehe auch--->)

Alt, Droge; Datentankstelle, Befähigung, Ernst I (geht aus dem Vorhandensein von Ernst II hervor, daher redundant); **Funktion, Hampelmänner** (zu gemein),

Lachen, Silikonkasten, Denken, Popel, Gerätekrake, aussaugen, Schlaf, Essen, Fotokopie/rer (wir wollten nicht in Wunden stochern)

An dieser Stelle möchten wir uns freundlichst bei unseren wissenschaftlichen Mitarbeitern Ulrike Wortmann und D.Ralondo bedanken.

Wir haben die Daten nun auf vielfältigste Weise aufbereitet. Uns interessierte wie weit die Realitäten von Soziologen, Künstlern und Wissenschaftlern auseinanderklaffen. Aus Kostengründen mußten wir ein vereinfachtes Verfahren anwenden, um weitgehend exakte Ergebnisse erzielen zu können. Wir stellten einen Antrag auf Stellung eines Hilfsmittel zur zahlenmäßigen Erzeugung von Realitäten. Bis dieser Antrag genehmigt wurde, ermittelten wir die Begriffe, mit denen wir repräsentativ arbeiten wollten (alphabetische Reihenfolge):

---

[3] "Luis Trenker" werteten wir als Konzentrationsnachlaß und haben die Befragung an dieser Stelle abgebrochen.

87,5% bezieht sich auf die Arbeit eines Soziologen, der eine Befragung unter Mailboxbetreibern vornahm. Er verschickte Fragebögen, von denen 24 Stück zurückflossen. (Der Rest geistert als Witz durch die Mailboxscene). Der Wissenschaftler stellte fest, daß 87,5% aller Mailboxbetreiber verheiratet sind (= 21). Besonders erschreckend war, daß der Herr mit dieser "Studie" seine Diplomarbeit gemacht hat....

Auftrag scheint zu sein, der Landesregierung einen Aufgaben- und Förderungsvorschlag im Bezug auf Computernutzung im Alltag vorzulegen. Falls nicht dieses ganze Projekt "Sozialverträgliche Technologien" lediglich ein Zinsbeschaffungsprojekt der Deutschen Bank (Staatsverschuldung) darstellt, denken wir, daß die Damen und Herren Wissenschaftler sich ein bißchen der Verantwortung ... bladröhnfasel...

Dinge werden immer ungerne beim Namen genannt. Künstler: "Das ist nicht das Ding, um das es geht..."

Eigenarten haben die Eigenart eigen-artig zu sein. Sie sind also nicht wissenschaftlich (denn Wissenschaft ist auf gar keinen Fall eigenartig) und somit nicht zu beachten. Eigenarten stören nur. ("Kind sei artig...)

"Sie werden lachen, wir meinen es **Ernst** II..."

Kaffee ist ein Getränk. Es wird getrunken. Mit Kaffee können sozialunverträgliche Theorien und praktische Ansätze etwas sauberer gewischt werden.

LebensWert ist ein schwieriges Wort. Es wurden auch Worte kreiert wie "Arbeitserleichterung" und "Sozialverträglichkeit". Bei Benutzung von Hilfsmitteln, und Worte sind nichts anderes, sollte man den Weg nicht zum Ziel machen. Auch nicht unwillkürlich.

Mädchen stehen der männlichen Betätigung als Anreiz vor Augen. Anstatt sich um flüchtige Erlebnisse zu prügeln, erwirbt der männliche Wissenschaftler seine Begattungspunkte durch seine Wissenschaft. [4] Von Ingolf Lück, dem bekannten Bielefelder Show-Talent soll das Gelübde ausgesprochen worden sein, daß er *alles* tun würde, um nicht körperlich arbeiten zu müssen...

[4] Ernst I

Möglichkeit. Allein schon die Möglichkeit zu haben, sich intensiv einer Sache widmen zu können, sollte zu einer gewissen Leistung befähigen. Sicher, Arbeit darf keinen Spaß machen, sonst wäre es Vergnügen und keine Arbeit[5] Aber vielleicht wäre es doch zuviel Anpassung, wenn man als tätsächlich ernsthafter Wissenschaftler, aus der Erkenntnis heraus, daß auf offiziellem Wege nur *Scheiße* wirkliche Würdigung (und Finanzierung) erfährt, die Selbstverleugnung soweit zu treiben, daß man als Profi nur noch eben jene *Scheiße* produziert. Und das Wichtige den Hobby-Forschern überläßt. Die Kunst (der Wissenschaft) liegt dazwischen. Nämlich dort, über den excellent abgefaßten Forschungsantrag hinaus (Kompliment Herr Rammert), auch die Wissenschaft dazu zu bringen, Forschung so zu betreiben, daß die Ergebnisse verwertbar sind. Wir werden das noch an einigen Beispielen ausführen. In Zukunft.

Musik. Wer nur etwas von Musik versteht, versteht auch davon nichts.[6]

Neugier ist nichts für Wissenschaftler. Sondern nur für Hobby-Forscher. Ein Wissenschaftler forscht nicht aus Neugier, sondern weil er einen Forschungsauftrag hat ('Die Pädagogisierung der Pädagogik" zum Beispiel). Siehe Oben. Unter 'Möglichkeit'.

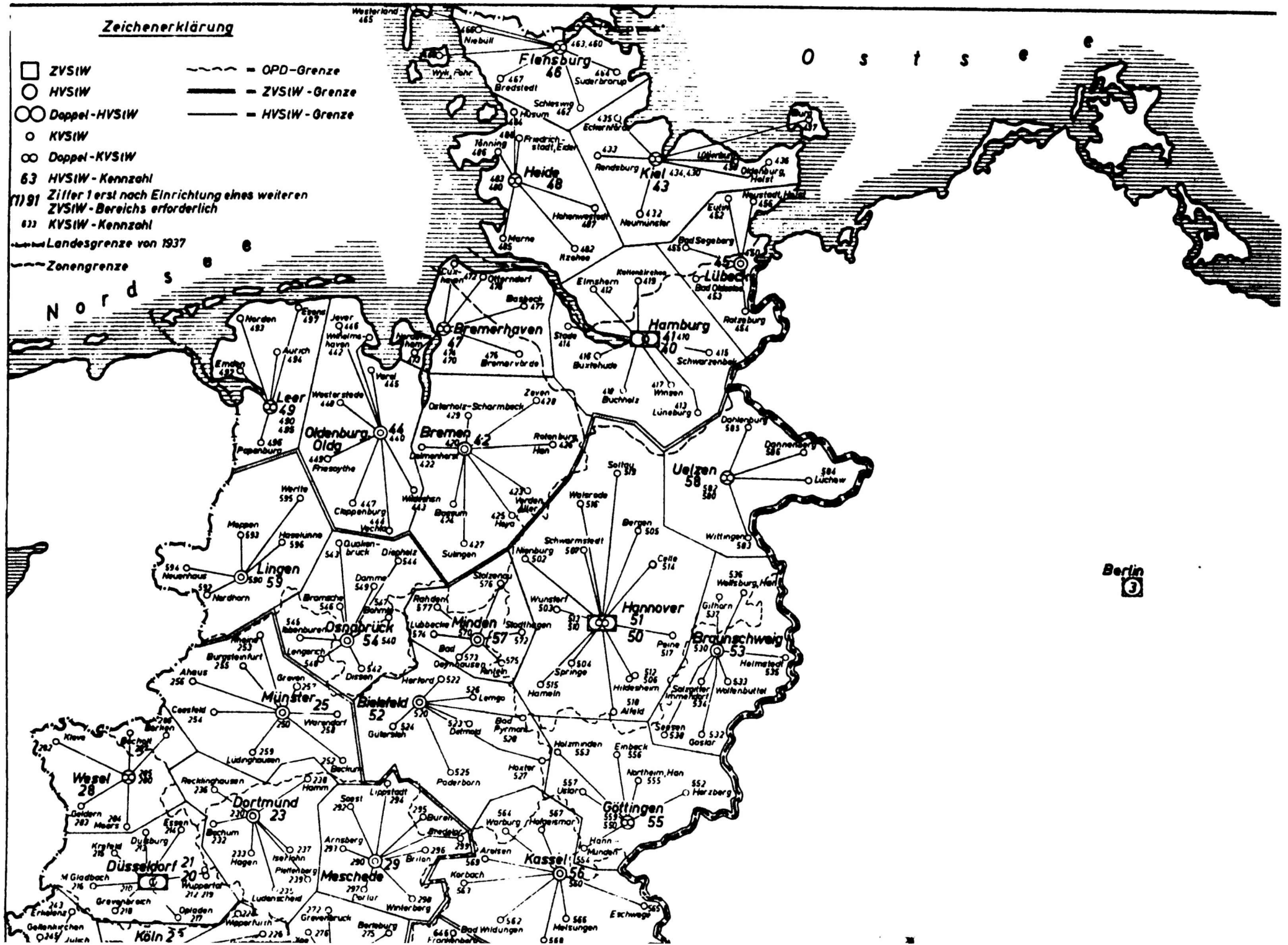
Programm. Was nicht im Programm steht, ist nicht Bestandteil der Veranstaltung / der Tagung / des Kongresses. (siehe 'Musik')

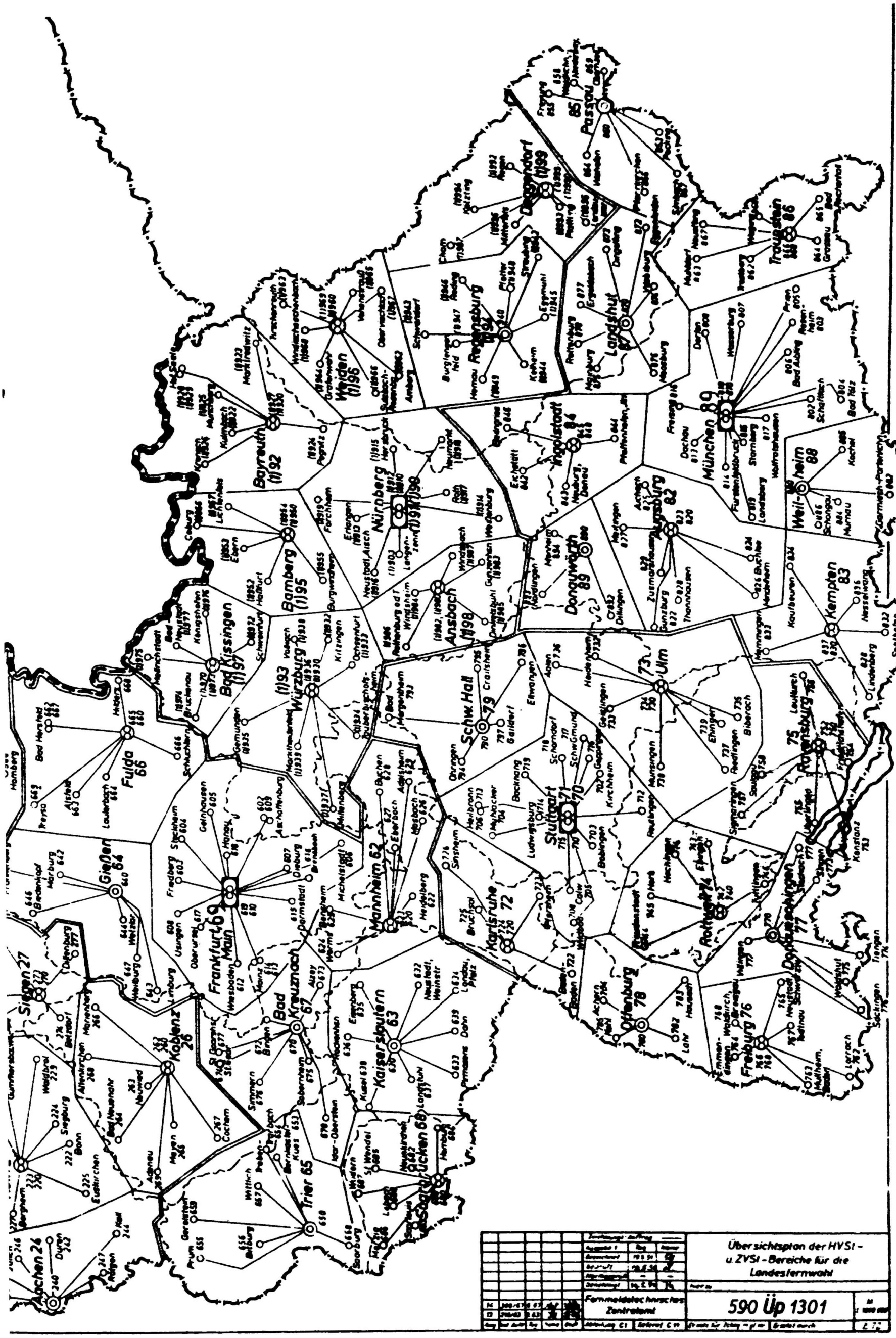
Tellerrand. Es ist schon ein Jammer, daß hier alles so streng nach Alphabet vorgehen muß. 'Tellerrand' würde so prima zu Worten wie 'Neugier', 'Programm', - ach zu fast allen Begriffen hier passen.

als Letztes: die **Zeit**. Die Zeit ist das, was man ohne es zu merken stets reichlich und zu wenig hat. Zeit lebt in enger Verbindung mit 'Möglichkeit' und 'LebensWert'. Zeit ist ewig, unendlich und unvergänglich. Zeit teilt sich diese Bezeichnungen mit Raum und Energie. Die Elemantarphysik hätte viel von der Germanistik, der Philosophie oder den Indianern übernehmen können. Einstein

[5] Theorie des Lager Messinghof, Kassel (Ltg.Prof.Rolf Lobeck)

[6] Erik Satie 1866-1925


Zeichenerklärung
ZVStW
HVStW
Doppel-HVStW
KVStW
Doppel-KVStW
63 HVStW-Kennzahl
(1)91 Ziffer 1 erst nach Einrichtung eines weiteren ZVStW-Bereichs erforderlich
633 KVStW-Kennzahl
Landesgrenze von 1937
Zonengrenze
OPD-Grenze
ZVStW-Grenze
HVStW-Grenze
Nordsee
Ostsee
Flensburg 46
Heide 48
Kiel 43
Lübeck 45
Bremerhaven 47
Hamburg 41 40
Leer 49
Oldenburg Oldg 44
Bremen 42
Uelzen 58
Lingen 59
Osnabrück 54
Minden 57
Hannover 51 50
Braunschweig 53
Münster 25
Bielefeld 52
Wesel 28
Dortmund 23
Düsseldorf 21 20
Meschede 29
Kassel 56
Göttingen 55
Köln 35
Berlin (3)


Becco 105.1070
Übersichtsplan der HVSt - u. ZVSt - Bereiche für die Landesfernwahl
Fernmeldetechnisches Zentralamt
590 Üp 1301
Passau 85
Regensburg 94
Landshut 87
München 89
Ingolstadt 84
Augsburg 82
Donauwörth 89
Ansbach 98
Nürnberg 98
Bayreuth 92
Bamberg 95
Würzburg 93
Bad Kissingen 97
Fulda 66
Gießen 64
Frankfurt 69
Mannheim 62
Karlsruhe 72
Stuttgart 70
Ulm 73
Kempten 83
Weilheim 88
Rosenheim 77
Freiburg 76
Offenburg 78
Schw. Hall 79
Kaiserslautern 63
Bad Kreuznach 67
Koblenz 26
Trier 65
Aachen 24
Siegen 27

Verschlüsselung für alle - PC-DES als CHARITYWARE

PC-DES Bestellungen (CHARITY-WARE) ganz einfach: DM 23,23 überweisen auf das Konto der Datenschleuder-Redaktion RN Nr. 86 23 04, BLZ 672 900 00, Heidelberger Volksbank. Versandadresse f. 5.25 MSDOS-Disk nicht vergessen! PC-DES als Charityware ist nur für den privaten Gebrauch von Einzelpersonen lizensiert; Gruppen, Inis u.ä. reden vorher mit uns. CHARITY-WARE ist durch Zahlung des Betrages oder (nachweislich) drei Stunden Arbeit für eine gemeinnützige Organisation (zB Weitergabe von Vernetzungs- und Computerwissen an Umweltinitiativen) lizensiert.

Die Redaktion dankt dem Autor, der die PC-DES-Charityware-Erlöse der Datenschleuder zur Verfügung stellt!

! Bei gewerblichem PC-DES-Einsatz ist eine (kommerzielle) Lizenz !
! zwingend erforderlich. Näheres bei BrainON!, Postf. 10 40 27, !
! D-69 HD. !

DS-RED-RN

hatte sich stets die Zeit genommen, um ein wenig mit seiner Frau zu streiten ...

Wir fassen die 14 Begriffe (2 * 7 Tage) noch einmal zusammen:

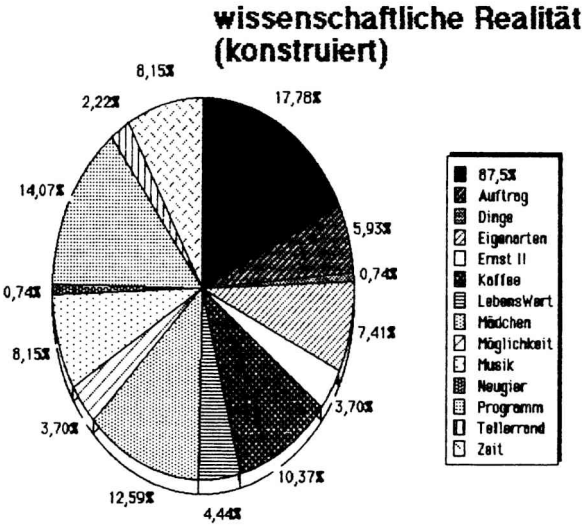
87,5%, Auftrag, Dinge, Eigenarten, Ernst II, Kaffee, Lebenswert, Mädchen, Möglichkeit, Musik, Neugier, Programm, Tellerrand, Zeit

Wir erhielten nun auch auch die Genehmigung uns wissenschaftliche Hilfsmittel zuzulegen. Der Etat war allerdings so bescheiden, daß er lediglich für den Kauf eines Ikosaeder (20-flächiger "Würfel") ausreichte. Wir haben also die Forschungsergebnisse nicht durch die Verfälschung von Realtitäten erzielt, sondern diese direkt ausgewürfelt. Lediglich der Wert '24' für den Begriff '87,5%' war vorgegeben (siehe oben).

Als erstes würfelten wir die Zahlenwerte aus, die von Soziologie-Wissenschaftlern zusammengetragen worden wären. Dies ergab folgende Werte:

87,5%...24	**Auftrag....8**	**Dinge.....1**
Eigenarten...10	**Ernst II....5**	**Kaffee...14**
LebensWert.....6	**Mädchen..17**	**Möglichkeit.....5**
Musik...11	**Neugier....1**	**Programm...19**
Tellerrand....3	**Zeit..11**	

Hier das Schaubild, mit der prozentualen Aufteilung

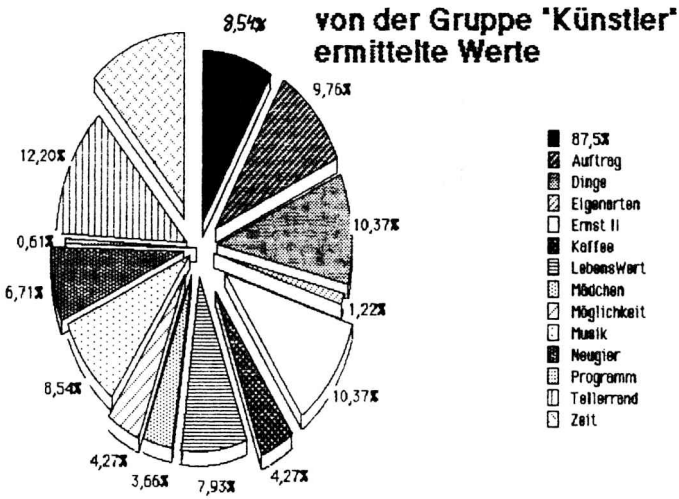


GRAFIK 1

Als zweites würfelten wir die Ergebnisse aus, die wir dem Bereich "Künstler" zuordneten. Über die Ergebnisse waren wir recht überrascht. Hatten wir - das mag verständlich sein - die Ergebnisse bei den Künstlern - von der subjektiven Warte aus - weitaus schmeichelhafter eingeschätzt.

87,5%..14	**Auftrag..16**	**Dinge..17**
Eigenarten....2	**Ernst II..17**	**Kaffee....7**
LebensWert..13	**Mädchen....6**	**Möglichkeit....7**
Musik..14	**Neugier..11**	**Programm...1**
Tellerrand..20	**Zeit..19**	

dies ergab folgende Grafik, deren Ausführung schon darstellt, daß Künstler nicht wissenschaftlich arbeiten können und somit stets an der Realität vorüberziehen:

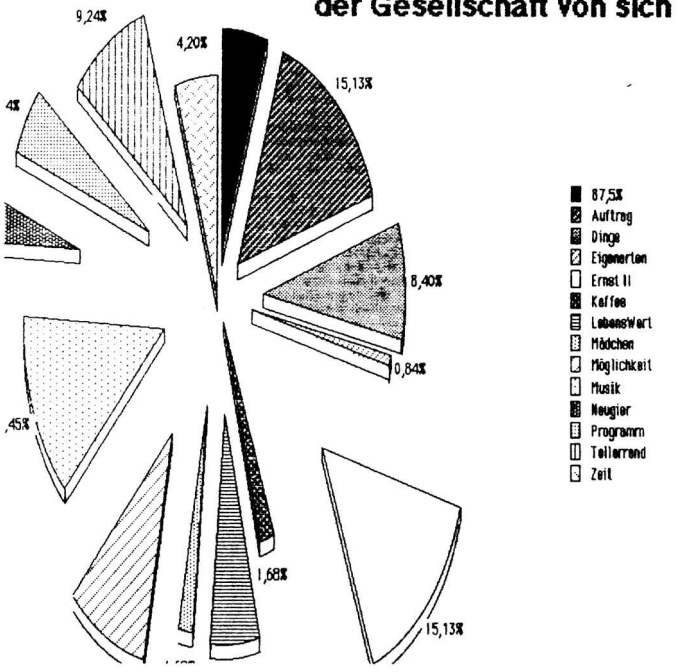


Grafik 2

Nun wollten wir auch noch durch repräsentatives Bewürfeln, Werte der allgemeinen (nicht-soziologischen und nicht-künstlerischen) Realität ermitteln.

Auch hierfür erschien uns unser Ikosaeder das geradezu phänomenal geeignete Arbeitsmittel zu sein. Er ist absolut unbestechlich und wenn man lange genug würfelt und die Ergebnisse mitschreibt... Sehen Sie, wie die Realtität aussieht. Natürlich hat die Realität keine Ahnung von der Wirklichkeit. Dies sehen wir an den fliegenden Tortenstücken der folgenden Tortengrafik:

die falschen Vorstellungen der Gesellschaft von sich selbst



GRAFIK 3

Aber auch hierzu die genauen Daten:

87,5%....6	**Auftrag..18**	**Dinge....10**
Eigenarten....1	**Ernst II..18**	**Kaffee.....2**
LebensWert....7	**Mädchen....2**	**Möglichkeit...11**
Musik..16	**Neugier....6**	**Programm.....6**
Tellerrand..11	**Zeit....5**	

ES IST NICHT UNBEDINGT VON BEDEUTUNG ABER WIR WOLLEN EIN PHÄNOMEN NICHT VERSCHWEIGEN. NACHDEM WIR DIE GESAMTSUMME JEDES BEGRIFFS GEZOGEN HATTEN UND AUCH DAVON EINE TORTENGRAFIKANFERTIGEN LIESSEN, STELLTE SICH - BEDINGT DURCH DIE GESETZE DER MATHEMATIK - EINE DEMOKRATISIERUNG DER UNTERSCHIEDE EIN. NACHFOLGEND - ZU IHRER INFORMATUION - DIE TORTENGRAFIK

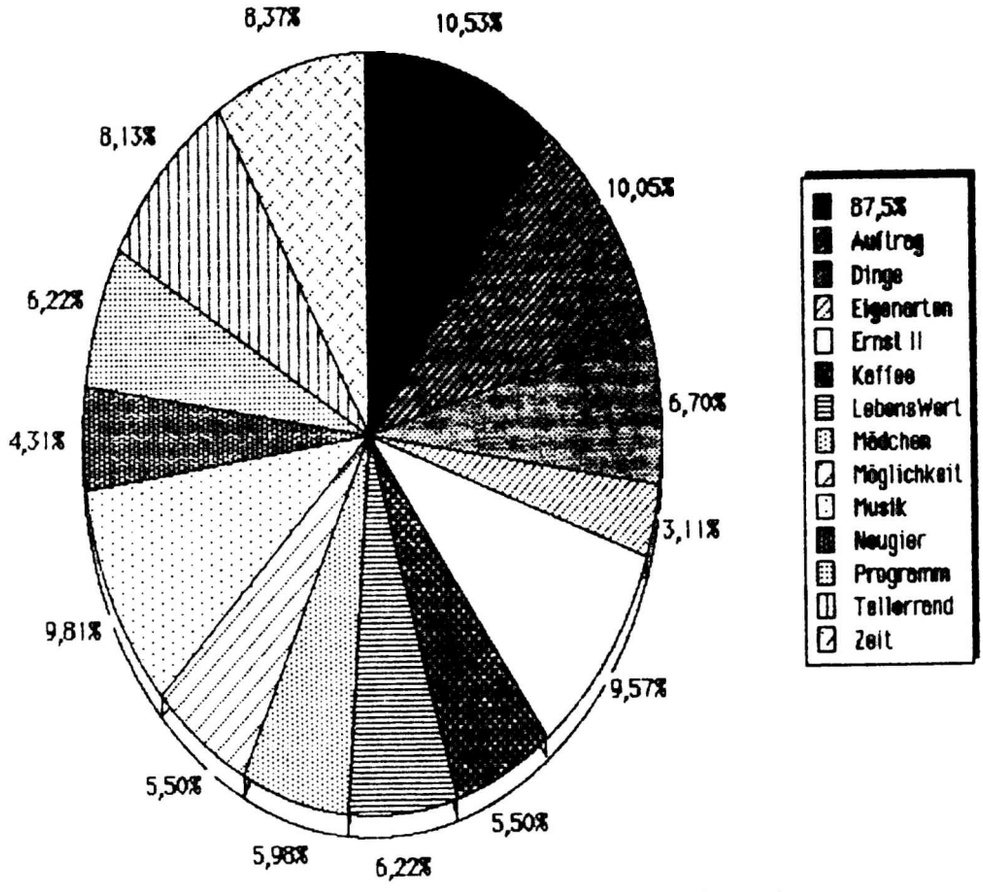


BILD 4

Da bleibt nur eins zu sagen:

Verisches Impressum

Die Datenschleuder (ds) ist ein selbstverlegtes Organ des Chaos Computer Club, einer galaktischen non-profit-corporation für Freie, Unbeschränkte, Chaotische Kommunikation (F.U.C.K).

Alle Beiträge und Geschichten sowie das allgemeine Erscheinungsbild spiegeln EinAnsichten der AutorInnen wieder und stehen nicht unbedingt in Widerspruch zu anderen Beiträgen. Die ds wird diffus kollektiv produziert und erscheint manchmal erst, wenn schon totgeglaubt. Diese Ausgabe wurde im Großraum Rhein-Necker-Bielefeld-(HH) mit unübersehbarer Unterstützung produziert. Zur aufgefrischten MitarbeiterInnenschar gehören - ohne Anspruch auf Vollzähligkeit neben unserem Schäf-Redaktor, der in Zukunft A.B.Geschafft ist, die locker-festen-freien terra, A.Eichler, B.Fix, P.Franck, Rena T., padeluun, M.Kühn, JWI, Andy, J.Nicolas, em, S.Werner, wau, die Bildschirmschänder der Sektion Passau und der Öblche unnennbare Haufen (wer hier fehlt oder gestrichen werden will: bitte melden!). Keiner wird dafür bezahlt außer den DruckerInnen (und die warten manchesmal aufs Geld, da Clubausgaben zumeist die Geldeingänge übersteigen - Danke für die Geduld!). Die Post dagegen verschickt die ds erst, wenns Porto bezahlt ist und belastet die ds finanziell am meisten.

Für das jetzige Erscheinen nach Monaten der Datenunterdrückung durch Bundeskriminale und andere schwach Sinnende ist verantwortlich ISd Presse Gesätzes Hervart Holland-Moritz. Den Druck besorgte die Hamburger St. Pauli Druckerei.

(Deix)-Hinweis: Das Titelbild wurde montiert aus >Mein Tagebuch<, Verlag Jugend und Volk, Wien, ISBN 3-224-16899-3. Anteile des in die Sprechblase montierten digitalisierten auf der CeBIT88 verteilten Bonbon von PHILIPS steht auf dem Deix'schen Original auf Seite 136 >APRIL! APRIL!< und als Bildtext >Der Innenminister kündigt eine Verbesserung der Polizistenausbildung an. Vermehrtes Schießtraining, psychologische Schulung und das Erlernen von Fremdsprachen stehen auf dem Programm.<

Da nach ORF-Recherchen in Österreich weder Hacker noch Hacken zu finden sind, gibt's einen Ö-TREFF auf den Chaos Communication Congress '88 in Hamburg; u. a. geht's um die Projektplanung eines Hackerbuches für Österreich mit Jugend und Volk.

Hinweis für AutorInnen: Mit der Einreichung eines Beitrages erhält die ds das Recht auf Abdruck des Beitrages in der ds sowie in der Hackerbibel im Rahmen der ds-Reprints. Logisch: Nach der Einreichung ist ein Verkauf des gleichen Beitrages an Dritte nur nicht-exkusiv möglich.

Adressübersicht in der nächsten ds! eMail: Z-Net (S.24/25) und GEO1:CHAOS-TEAM; dsred at RMIHD.uucp / CCC, Schwenckestr. 85, D-2000 Hamburg 20

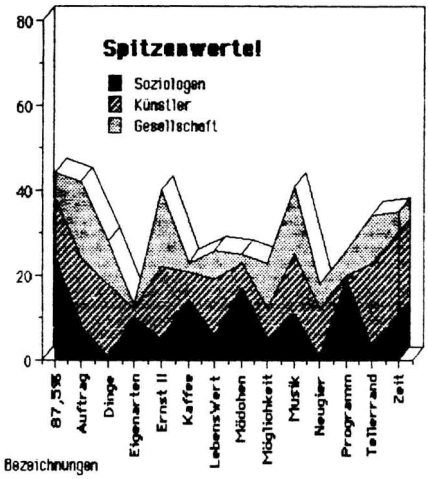


BILD 5

Ende des 1.Teils
Es geht weiter mit dem 2.Teil

ALLTAG, KUNST & COMPUTER
Was haben Soziologen damit zu tun?

Natürlich wird unsere Arbeit Fehler aufweisen. Das ist vollkommen klar und wir wollen das nicht beschönigen. Wir alle wissen, daß es vollkommen unmöglich ist, Menschen und Werte etc. korrekt zu erfassen. Wir denken, daß dies sogar zu den 15 Binsenweisheiten[7] gehört und somit gar nicht der weiteren

[7] Wahrheit ist wohlklingend - wohlklingende Worte sind nicht wahr.(Laotse).

Erwähnung bedarf.[8] Auch die Methode des direkten Auswürfelns von Ergebnissen ist noch heftig umstritten[9] Auch ist noch nicht endgültig geklärt, ob das Anfertigen von Grafiken die Richtigkeit von Daten herbeiführt. Der Auffassung von Michael Schirmer[10] nach ist dies legitim - solange es der Auftraggeber nicht bemerkt. Dem widersprechen Moralisten - wie zum Beispiel Wilhelm Busch[11,12]

Also wurden von uns die verschiedenen FehlerFaktoren berücksichtigt und wir haben den Spielraum grafisch aufarbeiten lassen:

---

[8] Diesen Teil können Sie selbstverständlich streichen. Logisch. Nicht wahr?

[9] Vergl.Bazon Brock: "Alles sitzt - alles paßt - zueinander."

[10] Werbeagentur GGK, Düsseldorf

[11] Diese Daten werden überarbeitet und sind zur Zeit nicht verfügbar.

[12] © für den text von Fußnote 10 bei DEUTSCHE BUNDESPOST (BTX-Standard-Text)

ZERBERUS-NETZ SYSTEMLISTE (Stand 1. Dez. 1988)

VWahl	TelNr.	Name /Standort	24h	Baud
0201	256885	Eloi's MailSystem Essen	J	2400
0202	473086	ToelleturmBox Wuppertal	J	2400
0202	463678	RonsdorferMailBox Wuppert	J	1200
0203	701806	Ibm User System Duisburg	J	2400
02051	21568	Vopatepatu Velbert	J	1200
02151	798202	LAB's Toenisvorst	J	1200
0221	244054	Silly's MailSystem Köln	J	1200
0221	558336	Links-Köln	J	1200
02203	25838	Atari Box Colongne Köln	J	1200
02236	63371	Magic Mountain Köln	J	1200
02241	404403	Midimail Troisdorf	J	1200
02324	52544	ComTopMailbox Hattingen	J	2400
02841	57325	Moerser Hacker Box	J	1200
040	4911085	Chaos Comp. Club (Hamb)	J	24!!
040	7687546	Harburger Datenkiste Hamb	J	1200
040	701950	Amiga Network Moorburg Hmb	J	2400
0551	59172	First Göttinger Mailbox	J	1200
05851	7896	Astronomie-MB Dahlenburg	N	1200
061103	45287	Bitmail Egelsbach	J	2400
06204	8521	Wildcat Viernheim OFFLINE	J	1200
06332	72417	GrossComp.Sys. Zweibrücken	J	1200
06753	5407	JesusOnLine Calbach	N	1200
06806	3978	UserMailSystem Saarbrücken	N	1200
0681	873240	Eierkocher Saarbrücken	J	2400
06831	41214	Links-Saarland Saarlouis	J	1200
0821	722166	Allg.Computerclub Augsburg	J	1200
089	1234456	Infoxx München	J	1200
089	3001426	BBPP München	N	300
089	397186	AHB-Wirtschatsdatenbank MO	J	1200
089	6519279	Infinet-München	N	2400
089	5706448	Links München	J	1200
089	72506629	GCN München	J	1200
089	8002993	Ravenna München	J	1200
0911	452777	Links-Nürnberg	J	300
0911	562368	AlphasoftMailBox Nürnberg	J	1200
09131	992998	ASK MailBox Erlangen	J	2400
004145	211488	Investra Kaltbach SCHWEIZ	J	1200
0043222744417		Phoenix Wien ÖSTERREICH	J	2400
--(24!! Keine 300)----------				-DS-RED-

KURZMELDUNG —— CLUBMAILBOX ——————————AKTUELL——————
Hamburg (CCC) - Seit dem 1. Dezember '88 betreibt der CCC sein eigenes Mailbox-Netz auf ZERBERUS-Systemen, die Aktivitäten auf der einsamen CLINCH-Box wurden eingestellt. Um die stark dezentralisierte Arbeit des Clubs und der Redaktion Datenschleuder wieder transparent zu gestalten, werden zunächst in Hamburg, Lübeck, Egelsbach und Heidelberg vernetzte Clubsysteme eingerichtet. Das Hamburger System 040-4911085 2400/1200 Baud und die BITMAIL 06103-45287 300-2400 Baud halten jeweils eine aktuelle Liste der angeschlossenen CCC-Systeme bereit. Zugang erhalten aus Kostengründen nur zahlende Mitglieder und/oder aktive Mitarbeiter/innen. Öffentliche Infos können als GAST abgerufen werden und sollen in Kürze auch auf dem ZERBERUS-Netz angeboten werden.
KURZMELDUNG —— HACKERBIBEL TEIL 2 ——————————————————
Heidelberg/Hamburg (CCC) - Die Hackerbibel Teil 2 >Das Neue Testament< ist seit zwei Monaten fertig. Das 260 A4 Seiten umfassende Werk ist über den Buchhandel ISBN 3-925817-24-7 , über das SERVICE-CENTER des CCC (Schwenckestr. 85, 2 HH 20 >SCHICK SCHECK 35,- DM<) oder BTX *SERVICE CENTER# erhältlich.
——————————————————————————DS-RED-HH——————

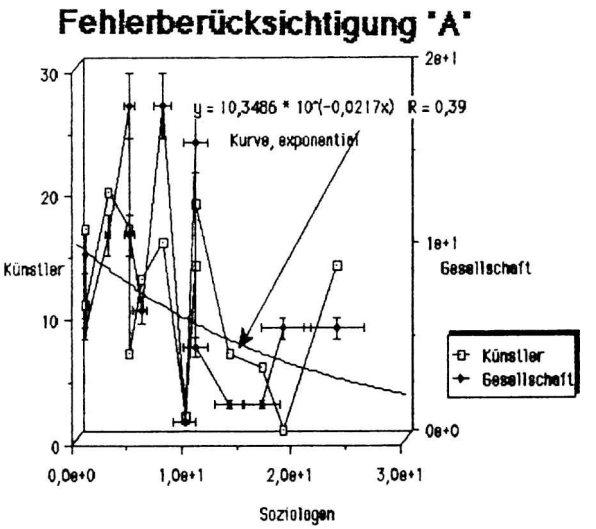


BILD 6

Was wir nun feststellen mußten, war, daß auch eine Fehlerberücksichtigung Fehler aufweisen kann. Außerdem erschien uns die Berechnungsformel noch nicht kompliziert genug: Zudem wollten wir die Sache auch von der anderen Seite betrachten.

Im folgenden (BILD 7) dokumentieren wir die Grafik von 'Fehlervergleich b':

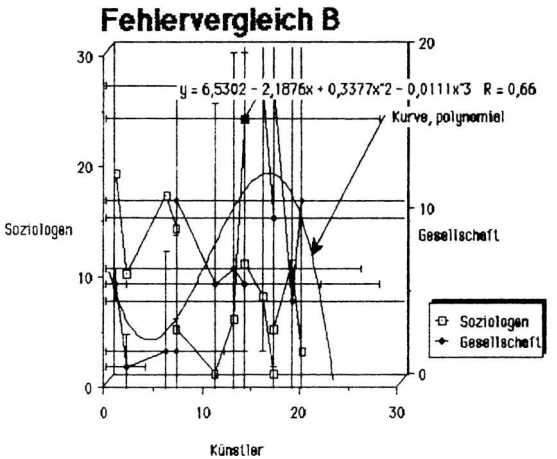


BILD 7

Zum Fehler noch einige Anmerkungen: "Der Fehler ist ein europäischer Zeitwert", sagte Mike A.Hentz[13]

Also ist - so gesehen - alles in Ordnung.

Alles ist gut.[14]

Alles ist Kunst.[15]

Jeder ist ein Künstler.[16]

Und wer sich dies zu Herzen nimmt und be-griffen hat, darf sich mit Fug und Recht Wolf Vostells "Jeder Mensch ein Kunstwerk" auf seine Steuererklärung schreiben. Und die Datenabgabe verweigern.

[13] Künstlergruppe: "minus DELTA t"

[14] Musikgruppe: "Deutsch-Amerikanische Freundschaft"

[15] Ives Klein

[16] Ja richtig. Das hat Josef Beuys gesagt. Vermutlich der einzige von den hier aufgeführten, den Sie kennen. Schade.

ALLTAG, KÜNSTLER & SOZIOLOGEN
Was haben Computer damit zu tun?

Computer - das wissen wir - verändern unsere Welt. Nicht nur die große - globale - Welt. Nein - gerade unsere kleine Allerweltswelt ist es, die in Mitleidenschaft gezogen wird. Darüber sind alle sehr froh[17]. Denn es geht voran.

Aber reden wir erst einmal über das Seltsamste:

Computer machen Menschen kompatibel.[18] Menschen, die normalerweise die Straßenseite wechseln würden, wenn sie sich begegneten, können plötzlich miteinander (über den Computer) kommunizieren. Der Computer (als Anlaß) führt zum Eigentlichen (dem Eigentlichen).

Das ist schön.

Friedlich stehen Nazis und Punks, Opas und Gummibärchen, Banklehrlinge und deren Chefs vor dem flimmerlosen Bildschirm und dem Schritt in eine neue aufregende Welt und fachsimpeln.

Das muß man erlebt haben.

In Mailboxen treffen sich Menschen, die daheim vor dem Computer sitzen und sich per Tastatur mit Menschen in anderen Kontinenten unterhalten. Die Standardsprache ist eine Art englisch. Abgesehen davon, daß man auf diese Art morgens um drei weiß, daß es in Singapur um 10 Uhr vormittags geregnet hat, klingt das revolutionäre daran nicht sehr einleuchtend.

Das muß man ausprobiert haben.

Es wurde sehr sehr viel negatives über Computer gesagt und geschrieben. Gerade von Wissenschaftlern. Aber eines übersehen Wissenschaftler gerne: Das Geld.

Es wurde in unserer Gesellschaft bisher vorausgesetzt, daß ein Mensch über eine **Wohnung**, ein **Auto**, ein **Telefon** und genügend **Kleidung** verfügte[19]. Dazu kommt nun noch der **Computer**. Ein weiterer Klotz am Bein, der am Fortkommen hindert.

Das muß man bezahlt haben.

---

[17] Anthony Hyman, THE COMING OF THE CHIP (Ein Chip wird kommen)

[18] Dafür gibt es wenig Kompatibilität zwischen einzelnen Computermodellen oder gar der Peripherie.

[19] Dazu gehört auch noch ein Bild auf dem Schreibtisch: Frau und Kinder.

Hier begeben wir uns in den Bereich der Wirtschaftswissenschaften und der Politologie. Wenn uns die Damen und Herren Soziologie-Wissenschaftler nun folgen würden, wären wir bald bei der Philosophie, Theologie, Telepathie, Mathematik, Kybernetik (Ihr merkt, wo's hinführt...?) und vielleicht sollten wir hier abbrechen. Denn es kann nicht unsere Arbeit sein, Eure Arbeit zu tun.

Unsere Arbeit ist KUNST.

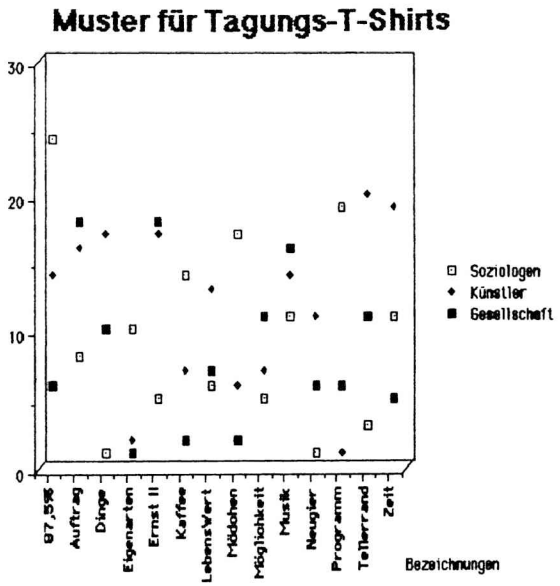
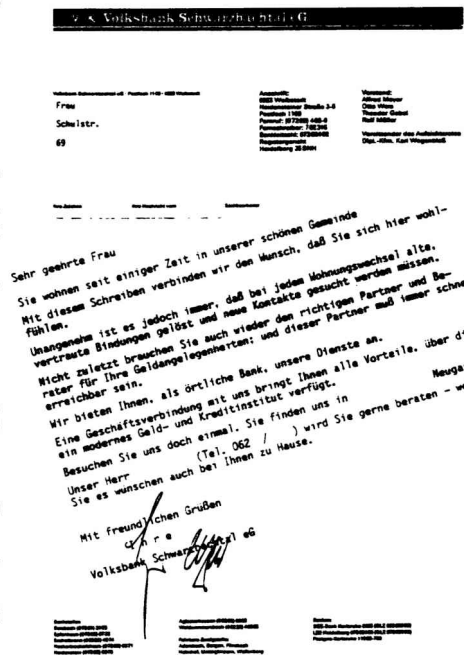


BILD 8

Einwohnermeldedaten an Bank weitergegeben

Gerade eingezogen am neuen Wohnort, einer 5000 Seelen-Gemeinde, erreichte uns das zum Abdruck anonymisierte Werbeschreiben einer Bank. Wie? Der Draht zum Wissen war das Telefon E. rief die Gemeindeverwaltung an:



Frau
Schulstr.
69

Sehr geehrte Frau

Sie wohnen seit einiger Zeit in unserer schönen Gemeinde

Mit diesem Schreiben verbinden wir den Wunsch, daß Sie sich hier wohlfühlen.

Unangenehm ist es jedoch immer, daß bei jedem Wohnungswechsel alte, vertraute Bindungen gelöst und neue Kontakte gesucht werden müssen.

Nicht zuletzt brauchen Sie auch wieder den richtigen Partner und Berater für Ihre Geldangelegenheiten: und dieser Partner muß immer schnell erreichbar sein.

Wir bieten Ihnen, als örtliche Bank, unsere Dienste an.

Eine Geschäftsverbindung mit uns bringt Ihnen alle Vorteile, über die ein modernes Geld- und Kreditinstitut verfügt.

Besuchen Sie uns doch einmal. Sie finden uns in Neugasse 5.

Unser Herr (Tel. 062 /) wird Sie gerne beraten – wenn Sie es wünschen auch bei Ihnen zu Hause.

Mit freundlichen Grüßen

Volksbank Schwarzbach eG

E.: Guten Tag, ich möchte bitte den hiesigen Datenschutzbeauftragten sprechen.

Gesprächspartner (G): WEN bitte?

E.: Den Datenschutzbeauftragten.

G: Haben wir hier nicht. Um was geht es denn?

E.: Nachdem wir uns angemeldet haben, erreicht uns unverständlicherweise als erste Post hier ein Werbeschreiben einer Bank.

G.: Ah ja, da verbinde ich Sie mit dem Einwohnermeldeamt.

Kleine Wartepause, dann meldet sich Frau R.

R.: Guten Tag, Sie wünschen bitte?

E.: Guten Tag, Frau R. Können Sie mir sagen, wie es kommt, daß die Volksbank von unserem Einzug hier erfahren konnte?

R.: Ja, das haben wir dorthin gemeldet.

E.: Wie? Ihre Dienststelle meldet meinen Umzug an eine Bank weiter?

R.: Ja, wir haben dafür die Erlaubnis des Bürgermeisters.

E.: Aber das geht doch wohl nicht. Das verstößt gegen den Datenschutz.

R.: Wir haben dafür die Erlaubnis. Aber ich gebe Ihnen dafür am besten den Bürgermeister.

Brgm.: Guten Tag, Herr E., was kann ich für Sie tun?

E.: Guten Tag, Herr Bürgermeister. Ihr Einwohnermeldeamt gibt Meldedaten an eine Bank weiter. Das verstößt gegen den Datenschutz.

Brgm.: Wir geben nur den Namen und die Adresse weiter, das verstößt nicht gegen den Datenschutz.

E.: Ah ja. Wie kann ich denn diese Informationen für meine eigene Firma bekommen?

Brgm.: Sie müssen ein berechtigtes Interesse vorweisen.

E.: Unser Interesse ist das gleiche, wir wollen auch Geschäfte mit diesen Leuten machen.

Brgm.: Das reicht uns nicht.

E.: Warum nicht, die Interessen sind doch dann die gleichen.

Brgm.: Bei der Bank ist das wohl etwas anderes.

E.: Wenn die Bank Kredite mit zwei bis drei Prozent Zinsen anbieten wollte, wäre das ein soziales Angagement erster Güte. Ein berechtigtes Interesse könnte ich dann auch einsehen. Aber hier handelt es sich doch um die solidesten Unternehmen, die mit interessanten Informationen aus Ihrem Amt versorgt werden, die wir für unsere Firma nicht bekommen können. Das widerspricht sogar eindeutig den Regeln der freien Marktwirtschaft.

Brgm.: Sehen Sie, das haben wir schon immer so gemacht. Und es hat sich bisher keiner darüber beschwert.

E.: Ja, dann frage ich noch einmal ganz ein-

deutig, kann ich für unsere Firma – sie will auch in Geschäftsverbindung treten mit neu Zugezogenen – die Namen und Adressen von diesen Leuten bekommen? Wir können dann Teppiche, Gardinen usw. anbieten.

Brgm.: Das geht wohl nicht.

E.: Wie, bei der Bank geht das doch. Sie haben das erlaubt!

Brgm.: Dort liegt auch ein berechtigtes Interesse vor.

E.: Nicht mehr oder weniger als bei uns auch.

Brgm.: Da gibt es wohl einen Unterschied.

E.: Einen Unterschied? Das kann ich nicht gelten lassen. Da bestehe ich dann besser auf meinem Datenschutz.

Brgm.: Sie sind der erste, der sich beschwert.

E.: Da muß ich entgegenhalten: der Innenminister Zimmermann steht auch hinter dem Datenschutzgesetz.

Brgm.: Ja, der Zimmermann, das Datenschutzgesetz hat der doch nur wg. der Volkszählung gemacht.

E.: Das stimmt hoffentlich nicht ganz. Tatsache ist doch, daß das Datenschutzgesetz es verbietet, daß Daten auch aus Verwaltungen weitergegeben werden. Und diesem Grundsatz müssen Sie doch erst einmal entsprechen.

Brgm.: Ja sicher, personenbezogene Daten. Aber wir geben doch nur die Namen und Adressen an die Bank.

E.: Es gibt immer mehr Menschen in Deutschland, die sich darüber aufregen, wie wir hier in der BRD, ähnlich wie in Rußland, uns an- und abmelden müssen. Also unsere Bewegungsfreiheit wird hier kontrolliert und überwacht. Und da melden Sie das sogar an eine Bank. Welches Interesse wird da berücksichtigt?

Brgm.: Die Bank hat ein berechtigtes Interesse. Die soll doch schließlich wissen, wenn Leute wegziehen und Verbindlichkeiten hinterlassen.

E.: ø ♥ ↑ ®®™ʒ ʒ ⌟ ♦ ⊣ æ {d Π
— ©⟨ œ '' m • - | ∂ ♣

Brgm: Ich verstehe Ihre Aufregung nicht. Sie sind wirklich der erste, der sich hier um seinen Datenschutz kümmert.

E.: Es ist doch so, es gibt ein Gesetz, gegen das Sie verstoßen, weil sich hier keiner drum kümmert. Es kann doch nicht angehen, daß ein Gesetz von der Verwaltungsseite her nur befolgt wird, wenn ein Bürger dasteht, der das kennt und sein Recht einklagt. Das Gesetz hat Allgemeingültigkeit, damit eben nicht jeder es immer wieder einklagen muß.

Brgm.: Gut. Wenn Sie darauf bestehen, werde ich das in Zukunft einstellen. Geben wir die Informationen nicht mehr weiter. Damit können wir das Gespräch dann beenden.

E.: Einen letzten Satz will ich dazu noch sagen. Für mich klingt jetzt heraus, daß Sie über eine neue Information verfügen, die mich betrifft und mich, eventuell, auch wieder einschränkt – in der Zukunft, meine ich. Sie wissen jetzt, daß ich ein „Verrückter" bin, der seinen Datenschutz einklagt. Ich möchte Sie als Bürgermeister darauf aufmerksam machen, daß Sie das vertraulich zu behandeln haben. Und, jetzt wirklich der letzte Gedanke, durch Ihr ungesetzliches Verhalten das einfache Gesetz 'Datenschutz' betreffend – dieser Schutz von Verwaltungsdaten sollte von Staatsbediensteten selbstverständlich anerkannt sein – stellen Sie den Inhalt dieses Gesetzes auf den Kopf. Anstatt daß der Datenschutz den unkontrollierten Fluß von Daten einschränkt, verfügen Sie nun, was mich persönlich betrifft, über ein weiteres Selektionskriterium. 'E.' verbirgt sich hinter seinem persönlichen Datenschutz. Ich möchte Sie bitten, darüber keine neue Datei anzulegen.

Brgm.: Ich verstehe Sie wirklich nicht. Es hat sich noch nie einer beschwert.

E.: Dann bin ich der erste. Und wenn es dazu beigetragen hat, daß diese Daten jetzt nicht mehr an die Bank weitergeleitet werden, hat dieses Gespräch sich ja gelohnt. Auch wenn Sie jetzt wissen, was ich für einer bin. Schönen Dank für dieses Gespräch.

Brgm.: Bitte, auf wiederhören.

E.: Auf wiederhören.

P.S. Es gibt auch eine zweite Bank am Ort ohne den Zusatz e.G., von der bis heute keine Werbung gekommen ist. Der Wettbewerb wird also tatsächlich verzerrt durch Vorteilsannahme der Bank e.G.

Gedächtnisprotokoll von E. am 10.8.1988

Chinesisch für AnfängerInnen

t'ung

sich frei ohne Behinderung bewegen; frei zirkulieren; **sich in unbehinderter Kommunikation befinden**; zu einer neuen Idee kommen; aufnahmebereit sein *(intransitives Verb)*

etwas zirkulieren lassen; **Kommunikation herstellen**; **etwas kommunizieren lassen** *(transitives Verb, kausativ)*

gut durchzirkuliert; erfahren; aufgeschlossen; offen (im Sinne einer „offenen Straße"); unversperrt; allgemein zutreffend; universell *(passives Zustandsverb)*

generell, universell, total *(Adverb)*

Ein enges Synonym ist ***ta***, aber eigentlich meint ***ta*** durch ein Medium brechen, das ein Hindernis darstellt, während ***t'ung*** ein Durchgehen durch eine Passage bedeutet, die kein Hindernis ist. ***ta*** tendiert dazu, das Erreichen eines Zieles zu betonen, wohingegen ***t'ung*** die Natur des Prozesses betont.

(aus *A First Course In Literary Chinese* von Harold Shadick und Ch'iao Chien, Cornell University Press, Vokabelband Seite 319f)

Syn ektik *(gr.) die*; - : das Studium von kreativen Prozessen von unterschiedlichen Gruppenmitgliedern zur Lösung von Problemen; vgl. Brainstorming (Duden 5,708)

12.3 Wie Chaos entsteht

Da wir die Variablen auf unterschiedliche Weise skalieren können, können die Lorenz-Gleichungen in verschiedener Gestalt auftreten. In diesem Abschnitt werden wir die folgende Form benützen

$$\dot{q}_1 = -\alpha q_1 + q_2\,, \tag{12.12}$$

$$\dot{q}_2 = -\beta q_2 + q_1 q_3'\,, \tag{12.13}$$

$$\dot{q}_3' = d_0' - q_3' - q_1 q_2\,. \tag{12.14}$$

Diese Gleichungen ergeben sich aus (12.3 – 5) durch die Skalierungsvorschrift

$$X = bq_1;\quad Y = \frac{b^2}{\sigma}q_2;\quad Z = r - \frac{b^2}{\sigma}q_3';\quad t = \frac{1}{b}t';$$

$$\alpha = \frac{\sigma}{b};\quad d_0' = r\frac{\sigma}{b^2};\quad \beta = \frac{1}{b}. \tag{12.15}$$

Der stationäre Zustand von (12.12 – 14) mit $\dot{q}_1, \dot{q}_2, \dot{q}_3' = 0$ ist durch

$$q_1^0 = \pm\sqrt{(d_0' - \alpha\beta)/\alpha},\quad q_2^0 = \pm\sqrt{\alpha(d_0' - \alpha\beta)},\quad q_3'^0 = \alpha\beta \tag{12.16}$$

gegeben. Die lineare Stabilitätsanalyse ergibt, daß die stationäre Lösung für

$$d_0' = \alpha^2\beta\cdot\frac{\alpha + 3\beta + 1}{\alpha - \beta - 1} \tag{12.17}$$

instabil wird.

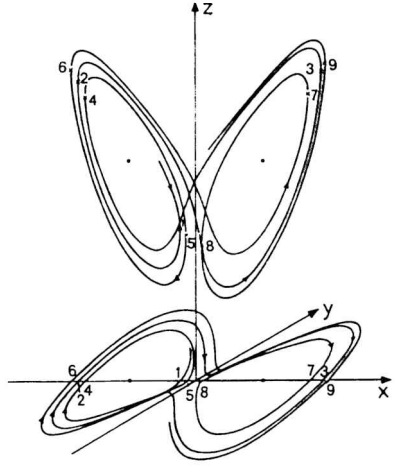


Abb. 12.2. Obere Hälfte: Trajektorien in der Projektion auf die (X, Z)-Ebene.
Untere Hälfte: Trajektorien in der Projektion auf die (X, Y)-Ebene.
Die Punkte gehören zu stationären Lösungen. Nach M. Lücke

Kurze Rezension
Synergetik ist die Lehre vom Zusammenwirken verschiedener Kräfte, deren Ergebnis mehr als die Summe der Einzelkräfte ist. *Lesetip*: Nebenstehendes Buch. Formelbeladen und spannend.

Titel der englischen Originalausgabe
H. Haken: *Synergetics. An Introduction.* (Third Revised and Enlarged Edition)

ISBN 3-540-12356-3 3. Auflage Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-12356-3 3rd edition Springer-Verlag New York Heidelberg Berlin Tokyo

ISBN 3-540-12597-3 2. Auflage Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-12597-3 2nd edition Springer-Verlag New York Heidelberg Berlin Tokyo

ISBN 3-540-11050-X 1. Auflage Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-11050-X 1st edition Springer-Verlag New York Heidelberg Berlin

CHAOS COMMUNICATION CONGRESS '88

Hamburg (CCC88/ORGA) Unter dem diesjährigen Motto "Ich glaub' es hackt!" veranstaltet der Chaos Computer Club (CCC) zwischen Weihnachten und Neujahr seinen inzwischen traditionellen Chaos Communication Congress. Zum 5. Mal treffen sich Hacker und Häcksen, Sysops, Datenreisende und Netzwerker zu ihrer internationalen Hackerparty in Hamburg zum Erfahrungsaustausch und zur Wissensförderung in der informierten Gesellschaft.

Elektronisches Akteneinsichtsrecht ist knapp 200 Jahre nach der Erringung des Bürgerrechtes auf Akteneinsicht (frz. Revol. 1789) eines der Diskussionsthemen. Vorgestellt wird als Ansatz für einen demokratischen Minimalstandard das "Freedom of Information Act". Informationelle Selbstbestimmung von Lebewesen ist mehr denn je nötig, wenn der Überblick über die Entscheidungsgrundlagen hergestellt werden soll.

Debattiert wird über Rechner- und Hausdurchsuchungen, Inhaftierung und den absurd-futuristischen Vorwurf eines Konzern an den Chaos Computer Club, Forschungsergebnisse der "nächsten zwanzig Jahre" aus einem Computer gestohlen zu haben.

Wichtige ordnungspolitische Fragen in der informierten Gesellschaft sind Regeln zur Datenöffnung mit dem Prinzip "Private Daten schützen - öffentliche Daten nützen".

Zum Thema "Fragen zur Ordnungspolitik in der informierten Gesellschaft" hat der Chaos Computer Club unter anderem den Hamburger Verfassungsschützerchef Christian Lochte, einen Vertreter der Staatsanwaltschaft und Fachleute aus Wissenschaft und Forschung geladen.

Spannend wohl auch das Theaterstück "Chaos im Computer Club" vom statt-Theater Neumünster. Das Kinder- und Jugendtheater der Naturfreundejugend Neumünster hat seine Sicht der Ereignisse um den Chaos Computer Club bühnenreif gemacht. Das Stück entstand unabhängig vom CCC - und so wird es auch für die Congressteilnehmer interessant werden, wie Aussenstehende das Wirken der Hacker empfinden.

Das eigentliche Kongressprogramm im Eidelstedter Bürgerhaus verspricht wie immer eine Vielzahl interessanter Themen. Auffällig ist, daß in diesem Jahr der Schwerpunkt auf inhaltliche Arbeit mit Computern gelegt wurde. Dazu gehören nicht nur Möglichkeiten der alternativen Computernutzung, sondern auch praktische Ansätze mit Bürgernetzen und öffentlich nutzbaren "Wissensdatenbanken". Unter dem Titel "Folgen der Informationsflut - Ebbe im Gehirn" wollen die Congressteilnehmer aber auch den Unterschied zwischen "Informationsgesellschaft" und einer informierten Gesellschaft herausarbeiten.

Die technischen Themen sind ebenfalls bürgerorientiert. Als Clou wird die Fertigstellung eines Verschlüsselungssystems für jedermann vorgestellt. Aktuelle Themen wie Viren, Würmer, Datex-P und der Einsatz von Mäusen stehen ferner auf dem Programm.

Ich glaub' es hackt!

Vom 28.12.88 12 Uhr
bis 30.12.88 16 Uhr

Eidelstedter Bürgerhaus,
Elbgaustraße 12, 2000 Hamburg 54

Teilnahme

Mitglieder des CCC e.V.	20.-
Private Teilnehmer	30.-
Presse	50.-
Gewerbliche Teilnehmer	100,-

In der Congressteilnahme sind sämtliche Rahmenveranstaltungen in der Markthalle (Podium & Theater) und der persönliche Kongressausweis enthalten. Bitte passendes Foto mitbringen!

Rahmenprogramm

Ich glaub' es hackt!
FRAGEN ZUR ORDNUNGSPOLITIK IN DER INFORMIERTEN GESELLSCHAFT

Podiumsdiskussion am 29. Dez. 1988 15h Markthalle / Klosterwall Eintritt für Gäste DM 6,- (In der Congressteilnahme enthalten).

HOCHPOLITISCH UND GANZ SCHON GRUSELIG - Hacker von Konzern entführt!

CHAOS IM COMPUTERCLUB - Theaterstück der Naturfreundejugend Neumünster am 28. Dez 19.00 h Markthalle (Klosterwall)

Eintritt (VVK)	Kinder bis 13 J.	5.50 DM
	Erwachsene	7.70 DM
Abendkasse	Kinder bis 13 J.	8.-- DM
	Erwachsene	10.-- DM

Der Zutritt ist in der Congressteilnahme enthalten!

Voranmeldung

Durch Einzahlung auf das Postgirokonto des CCC in Hamburg Kto. 59 90 90 - 201 (BLZ 20010020) Stichwort: CCC88 (Bitte Beleg mitbringen!)

Karten für das Theaterstück bei allen bekannten Vorverkaufsstellen!

Übernachtung

Bisher sind zwei Jugendhotels gefunden. Beide kosten ca 30,- DM je Nacht. Preiswerter ist es nur bei Freunden.
Kontakt: ESCO 040 - 31 06 59
Club 040 - 490 37 57

Referenten & Helfer

Wer noch aktiv am Congress mitarbeiten will kann ab 26. Dez. 10 Uhr anreisen, oder sich bei Steffen 040 - 483752 melden.

Kontakt

Vorher	
CCC-Hamburg:	040 - 490 37 57
DS-RED/RN:	06226 - 43 52 (FAX 40047)
Orga-Team:	040 - 48 37 52
Congress	
Projektleitung:	040 - 570 29 72
Pressestelle:	040 - 570 29 92