Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 83 (2005)

Heft: 5

Artikel: Teile und herrsche : Digital Divide

Autor: Klipstein, Deland L.

DOI: https://doi.org/10.5169/seals-877154

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 15.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Teile und herrsche – Digital Divide

DELANO L. KLIPSTEIN **Wenn es einen Megatrend für die Informations- und Kommunikations (ICT) Branche in den nächsten fünfzehn Jahren gibt, dann ist es die Vernetzung: Alles und jedes steht elektronisch miteinander in Verbindung. Die Gesellschaft wird durch die «Überallkommunikation» verändert und gespalten: in solche, die diese Veränderungen mitmachen (können) und jene, die dazu nicht in der Lage sind. «Digital Divide» nennen das die Fachleute.**

Hier sind einige Felder, die unsere Gesellschaft prägen werden. Sie ziehen Folgetechnologien nach sich, ohne die solche Veränderungen nicht greifen:

- Der «Digital Divide» kann die Gesellschaft spalten. Wer Zugang hat und die digitalen Medien zu nutzen weiss, gehört zu den Gewinnern. Wer draussen bleibt, wird Verlierer sein.
- Der E-Commerce wird zu einem Angebot, das über den Zweck des Einkaufs hinweg eine Art «interaktive Unterhaltung» wird. Callcenter werden rund um die Uhr ihre Dienste anbieten.
- «Ubiquitous Computing» wird zunächst im Warengeschäft zu Logistikzwecken, später dann auch im persönlichen Umfeld für mehr Bequemlichkeit eingesetzt.

Bild 1. Telefonieren scheint beim Handy in den Hintergrund zu treten. Moderne Mobilfunkgeräte vereinen viele Dienste unter einem Dach, so auch die Ortsfindung mit GPS. Von wo das Gespräch, die Anfrage, das Foto kommt, kann leicht örtlich zurückverfolgt werden. *Siemens AG*

- Automatische Übersetzungssysteme erleichtern die Kommunikation auch in seltenen Sprachen.
- Neue Technologien erfordern und ermöglichen mehr persönliche IT-Sicherheit.

Um dies zu realisieren, müssen existierende Technologien weiterentwickelt werden:

- Die weltweite Verbreitung der digitalen Medien macht auch weltweite Normen erforderlich. Hoher Nutzungswert von Standards beschleunigt die Einführung.
- Um die Netzbelegungszeiten nicht ausufern zu lassen und den elektronischen Verkehr zu beschleunigen, sind Breitbandnetze unabdingbar.
- Netzstrukturen werden sich verändern: Selbstorganisierende Netze und solche, die der Nutzer organisiert, werden dominieren. Endgeräte werden auch als Netzknoten dienen.
- Angesichts des schnell wachsenden Wissens wird Wissensmanagement grosser Informationsmengen mit Computerhilfe zu einem boomenden Geschäft.

Wir kommunizieren mehr elektronisch als persönlich

Das Handy und der PC mit seinen E-Mails wurden zum Symbol einer allzeit erreichbaren Gesellschaft. Damit verbunden verändern sich auch die Gesellschaftsstrukturen: weniger individuelle Kontakte, mehr elektronische Kommunikation.

Im Geschäftsverkehr hat das noch weitere Auswirkungen: Reisen treten zurück, Videokommunikation und E-Mail-Nutzung nehmen zu. Das alte Postfach wird ausgedient haben. Die Nutzung elektronischer Medien ist eine Basis für Erfolg im Beruf, Zeit- und Kostenersparnis sind die Triebfedern. Während heute unterschiedliche Standards durch Software angepasst werden, müssen sie in Zukunft durch frühzeitige internationale Vereinbarungen normiert werden. Insellösungen gehen zurück, es sei denn, ein dominierender Marktführer setzt die Standards durch die normative Kraft der Fakten.

Zu einem ernsten Problem könnte die digitale Spaltung der Gesellschaft führen. Dies trifft sowohl auf die Jungen, als auch auf die Alten zu. Trotz Computerunterricht in den Schulen nimmt die Zahl der «elektronischen Analphabeten» eher zu: Jugendliche, die nur unzureichend mit den elektronischen Medien umgehen können. In einer «elektronischen» Welt werden sie Schwierigkeiten haben, einen Arbeitsplatz zu finden. Ähnliches gilt auch für Ältere im Lauf ihrer beruflichen Tätigkeit. Wer sich nicht laufend weiterbildet, verliert den Anschluss und fällt aus dem Arbeitsangebot. Die gesellschaftlichen Konsequenzen sind hier

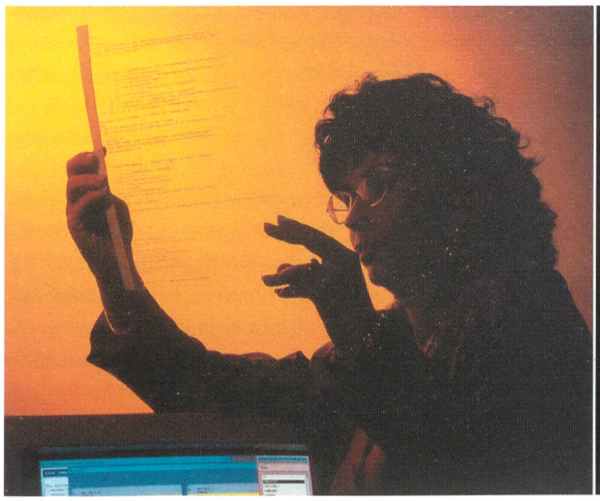

Bild 2. Die Hardwarekosten moderner IT-Geräte sinken unaufhaltsam weiter, auch wegen sinkender Halbleiterkosten. Die Softwarekosten hingegen steigen und bestimmen längst den Preis der Geräte. Bis zu 80% der Systemkosten gehen heute schon auf das Konto «Software». *Siemens Corp.*

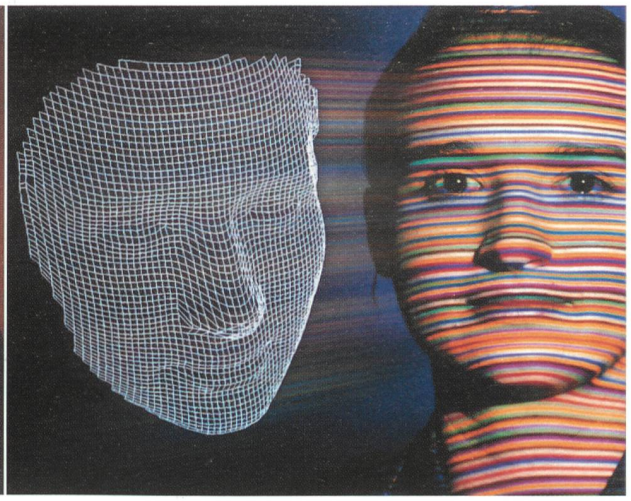

Bild 3. Mehr noch als Fingerabdrücke ist die Gesichtserkennung geeignet, die Identität einer Person zu sichern. Während links im Bild ein Rasternetz über das Gesicht gelegt und ausgewertet wird, nutzt man rechts im Bild farbige Linien und deren Verlauf zur Speicherung der personenbezogenen Daten. *Siemens AG*

noch nicht einmal skizziert, geschweige denn vorbereitend aufgegriffen.

Der Umgang miteinander wird unpersönlicher. Die Zahl der versendeten Short Messages (SMS) bei Jugendlichen liegt schon weit über der Zahl der Handy-Gespräche. Und auch E-Mails mindern den Griff zum Telefon. Die «Bildschirmkommunikation» führt zu rasant steigendem kommerziellem Missbrauch durch «Spam», unerwünschte E-Mails, deren schiere Masse bereits zu einem Kostenfaktor für die Server der Anbieter geworden ist.

Weitere Veränderungen kommen durch Informationsaustausch mit «anfassbaren» Service-Robotern und Software-Agenten. Dies kann auch zwiespältig gesehen werden, da zwar der Zuwachs an Bequemlichkeit und Perfektion als positiv empfunden wird, negativ dabei aber der Verlust an Privatsphäre ist. So lässt sich aus einem Handy-Anruf ohne grosse Schwierigkeiten rückrechnen, aus welcher Gegend der Anrufer sein Mobilgespräch führt. Wer über ein GPS-Handy verfügt, kann sogar punktgenau geortet werden (Bild 1).

Insgesamt wird die Rolle der Software in der IT-Technik (Bild 2) im Markt noch weiter zunehmen, die Bedeutung der Hardware rückläufig sein.

Selbstorganisation statt hierarchischer Ordnung

Früher einmal waren die Telefonnetze staatlich. Das sind sie heute nur noch in wenigen Ländern. Der hierarchische Aufbau dieser Netze machte die Verwaltung dieser Netze nicht sehr aufwändig. Doch seit der Erfindung des World Wide Web durch Tim Berners-Lee haben hierarchische Netze kein Monopol mehr. Selbstorganisierende Strukturen, die bei Bedarf entstehen und anschliessend wieder gelöst werden, haben ihre Rolle zum Teil übernommen. Das «Internet» ist physikalisch nicht greifbar: Es ist ein Softwarenetz, das sich zwar physikalischer Bausteine bedient, aber nur für die Dauer einer Verbindung real greifbare Strukturen zeigt.

Hier werden weiterhin grosse Veränderungen zu erwarten sein. Selbstorganisierende Netze sind dezentral, Endgeräte werden zu Netzknoten, Geräte unbeteiligter Dritter werden beim Aufbau von Adhoc- und Peer-to-Peer-Verbindungen miteingebunden. Nur noch der unmittelbare Nutzer – als Teilnehmer im Netz – hat eine Kontrolle darüber. Natürlich werden die alten Netzstrukturen nicht überflüssig, sie sind so etwas wie das Rückgrat des Welt-Kommunikationsnetzes. Doch damit sind auch die Haupteinsatzfelder für selbstorganisierende Netze gekennzeichnet: Im lokalen und regionalen Bereich zeichnen sie sich durch hohe Flexibilität und Effizienz aus.

Selbstorganisierende Netze haben auch ihre Probleme. Sie werden nicht von Betreibern betreut, sondern von den Anwendern jedes Mal neu aufgebaut. Ihre Qualität steht und fällt mit der Leistungsfähigkeit der Teilnehmergeräte, was Sicherheitslücken wahrscheinlich macht. Wer dies nicht akzeptieren kann oder will, ist weiter von der Netzinfrastruktur der überregionalen Anbieter abhängig. Dies gilt besonders bei weltweiter Kommunikation, da selbstorganisierende Netze hier nicht die nötige Stabilität erreichen.

Mehr elektronische Sicherheit für den Einzelnen

Wenn es in Zukunft ein boomendes Geschäft geben wird, dann liegt dies im wachsenden Sicherheitsbedürfnis des Menschen. Viel spricht dafür, dass sich der Staat aus manchen sicherheitsrelevanten Gebieten zurückziehen wird. Nur dort, wo das staatliche Interesse überwiegt – beim

«Horizons 2020»

Im Rahmen des von Siemens initiierten Zukunftsszenarios «Horizons 2020» wird ein Blick in die Zukunft der Information und Kommunikation (IK) geworfen. Die Expertenanalysen wurden in der Zentralabteilung «Corporate Technology» (CT) der Siemens AG von Dr. Hildegard Wiggenhorn zusammengefasst. Ergänzt wird dieser Bericht mit einem Interview mit dem Chef der IK-Division der Corporate Technology, Hartmut Raffler, und einem Laborbericht über «Sicherheit vor Seitenkanalattacken».

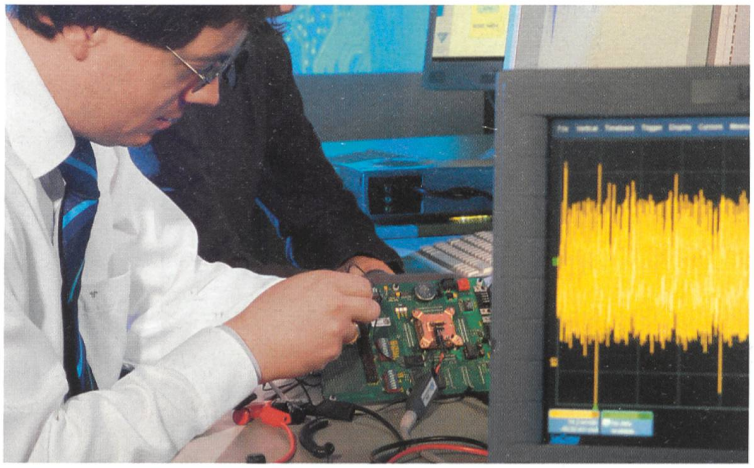

Bild 4. Extrahiert man aus Baugruppen so konventionelle Informationen wie den zeitlichen Ablauf des Stromverbrauchs oder den Verlauf der elektromagnetischen Strahlung während des Ablaufs kryptografischer Operationen, kann man statistische Rückschlüsse auf die verwendeten Verschlüsselungsverfahren ziehen. Im Labor von Siemens wird an Verfahren zur Abwehr solcher «Seitenkanalattacken» gearbeitet. *Siemens AG*

Schutz der eigenen Grenzen, in der Strafverfolgung, bei der Bekämpfung des internationalen Terrorismus – werden weltweite Lösungen dominieren. Private Anbieter werden die Lücken ausfüllen und umfangreiche Dienstleistungsangebote erbringen.

Dies gilt natürlich nicht nur für die «physische» Sicherheit, sondern auch für den Informations- und Persönlichkeitsschutz in einer elektronischen Welt. Dass dies dringend erforderlich sein wird, zeigen heute schon die Diebstähle von elektronischen Personenprofilen durch «Phishing», das vor allem in schwächer regulierten Staaten wie den USA oder Grossbritannien zu einer Bedrohung der Gesellschaft wird. Hochprofessionelle Sicherheitskontrollen, beispielsweise mithilfe biometrischer Merkmale, können nicht nur physikalischen Zugang sichern, sondern im Bedarfsfall auch den Zugriff zu Netzdaten (Bild 3).

Wie man gegen raffinierten Datendiebstahl vorgeht

Siemens hat in seinem Forschungslabor in München-Perlach kürzlich ein neues Labor eröffnet, das den Kampf gegen Hackerangriffe vor allem bei mobilen Endgeräten und «Embedded Systems» angeht. Dazu werden Implementierungen kryptografischer Algorithmen entwickelt, die für einen möglichst gleichmässigen Verlauf der mathematischen Prozesse auf dem jeweiligen Rechner sorgen.

Denn bei den so genannten «Seitenkanalattacken» versuchen Hacker gar nicht erst, die Logik hinter der Verschlüsselung zu knacken. Die Hacker greifen nicht die kryptografischen Algorithmen an, sondern nutzen unvermeidliche Nebeneffekte der verwendeten Hardware als Quelle. Da wäre zum Beispiel die direkte Änderung des Stromverbrauchs während der Durchführung einer einzelnen kryptografischen Operation. Oder die statistische Auswertung von Laufzeitschwankungen mehrerer aufeinander folgender Berechnungen.

Wir haben das Labor besucht und Laborleiter Dr. Erwin Hess hat uns die Arbeiten ein wenig aufgeschlüsselt. Durch statistische Auswertung des zeitlichen Verlaufs des Strombedarfs lassen sich Hinweise auf den Kryptoschlüssel gewinnen. Die Auswertung elektromagnetischer Strahlung während einer kryptografischen Operation liefert nutzbare Informationen, und selbst fehlerhafte Berechnungen auf dem betroffenen Chip kann man ausnutzen, wenn man den Fehler aktiv selbst provoziert. Die mathematische Statistik ist bei diesen Arbeiten ein unentbehrliches Hilfsmittel, als «Arbeitshardware» braucht man kaum mehr als ein hoch auflösendes Speicheroszilloskop und einen gut ausgestatteten schnellen PC mit geeigneter käuflicher Software. Korreliert man alle diese physikalischen Nebeneffekte miteinander, kann man bei mässigem Aufwand Rückschlüsse auf den verwendeten Kryptoschlüssel ziehen.

Wer glaubt, das wäre alles eine nette Spielwiese für Forscher, liegt völlig falsch: Wie einfach so etwas sein kann, demonstrierte Udo Helmbrechts, Präsident des deutschen Bundesamts für Informationstechnik, bei der Einweihung des neuen Forschungslabors. Er analysierte eine Baugruppe mit gespeichertem kryptografischem Schlüssel in einem Speicheroszilloskop. Nach kurzer statistischer Analyse der «Nebeneffekte» lagen die verschlüsselten Informationen offen (Bild 4). Die Wissenschaftler konnten nach 50 bis 200 Messungen erfolgreiche Attacken demonstrieren. Ihre eigentliche Aufgabe liegt nun darin, Systementwickler zu beraten, um solche Attacken unmöglich zu machen. ■

Absolute Sicherheit gibt es nicht

In der Corporate Technology von Siemens wird nach weiteren Implikationen für die Zukunft der IT-Technik geforscht. In einem Gespräch mit Hartmut Raffler, Chef der Division «Information und Kommunikation», haben wir die potenziellen Entwicklungfelder näher ausgeleuchtet.

Herr Raffler, betrachtet man die Entwicklungen in der Informations- und Kommunikationstechnik, dann drängt sich der Verdacht auf, dass die Triebfeder dahinter «Ubiquitous Communication» ist. Sehen Sie darin den grosse IT-Trend bis 2020?

Der Begriff «Ubiquitous Communication» ist schon etwas abgestanden: Er stammt von Xerox PARC, heute würde ich lieber von «Ambient Intelligence» sprechen: von Systemen, die den Nutzer in den Vordergrund stellen. Dahinter muss eine «Knowledge Base» stehen, eine Wissensbasis, die – auf den Nutzer bezogen – lernfähig ist und die Intensionen des Nutzers erkennt. Neuronale Netze werden diese Lernfähigkeit unterstützen.

Der Futurologe Ian Person von der British Telekom hält für die Zukunft sogar einen «physisch spürbaren elektronischen Händedruck» für denkbar. Ist «Fühlen» eine Richtung, in die sich die Informationstechnik in Zukunft bewegen wird?

Wir werden sicher in Zukunft neue Kommunikationsformen nutzen. Die bisherige Mensch-Maschine-Interaktion wird sich zur Mensch-Maschine-Kommunikation entwi-

ckeln. Als nächste Schritte sehen wir Kommunikation nicht nur mit Sprache, sondern auch mit Gestik, Mimik und Emotionen. Menschliche Kommunikationsformen spielen also in Zukunft in der Kommunikation mit technischen Systemen eine wichtige Rolle.

Ian Person spricht von «halbdurchlässigen digitalen Blasen», in denen der Mensch lebt, die unerwünschte Botschaften aussperren, wichtige Information aber durchlassen. Wie will man solche «Filter» bauen?
Das wird auf die Realisierung eines «semantischen Webs» hinauslaufen. In diesem werden die digitalen Inhalte durch semantische Anmerkungen angereichert. Dadurch kann gezielt auf die Interessengebiete des Individuums zugegriffen werden, verschiedene Inhalte lassen sich zu neuen Informationen kombinieren. Die Semantik ist entscheidend: Formale Grammatikregeln reichen nicht.

Zwischen der Hacker-Szene und den IT-Forschern gibt es seit Jahren ein Katz-und-Maus-Spiel: Jede noch so raffinierte Softwaretechnik konnte nicht verhindern, dass der Umfang von IT-Missbrauch weiter anstieg. Wächst der Aufwand für «Cyber Security» überproportional mit der Komplexität künftiger Systeme?
Wir hängen bereits heute in hohem Umfang von der Netzwerkkommunikation ab, ohne dass es die Öffentlichkeit wahrnimmt. Kraftwerke werden ferngesteuert, Flugzeuge finden ihren Weg mit dem Autopiloten, Züge fahren unbemannt. Kein Zweifel: Wir müssen die elektronische Infrastruktur noch sicherer machen. Bei Siemens in der Forschung besitzt das Thema «IT-Security» einen besonders hohen Stellenwert. Ein Beispiel dafür ist das Labor zur Abwehr von «Seitenkanalattacken».

In den USA will das neu gegründete TRUST-Konsortium (Team for Research and Ubiquitous Secure Technology) inhärent sichere Software schaffen. Kann man das überhaupt? Lässt sich fehlerfreie und unangreifbare Software entwickeln?
Bei vielen «Embedded Systems» kann man beispielsweise mathematisch verifizieren, dass eine gestellte Aufgabe erfüllt wird, die Software also fehlerfrei arbeitet. Bei grossen komplexen Systemen hingegen wird das schon schwieriger. Wichtig sind ausgefeilte, standardisierte Software-Entwicklungsprozesse, die durch qualitätssichernde Massnahmen begleitet werden. Notwendig sind auch Software-Architekturen, welche die Wiederverwendung von Software-Komponenten fördern. Absolute Sicherheit gibt es nicht, da im Lauf der Nutzung auch neue, bis dahin unbekannte Sicherheitslücken entdeckt werden, die dann schnell geschlossen werden müssen.

Automatische Sprachübersetzung hat in Papierform an Bedeutung gewonnen, wird auch in grösserem Umfang in eng begrenzten Gebieten wie der Medizin und der Rechtskunde eingesetzt. Sprachübersetzung in Echtzeit – für das Telefon zum Beispiel – scheint aber noch in weiter Ferne zu liegen. Wo liegt das Problem?
Im Gegensatz zu «Diktiersystemen», die das gesprochene Wort verlässlich in Text umwandeln sollen, kommt es bei der

Hartmut Raffler, Chef der Division für Information und Kommunikation im Forschungslabor der Siemens AG in München: «Die Entscheidung, welche Invention man vorantreiben will, wird auch in Zukunft nur der Mensch treffen können.» *Knapp*

verbalen Kommunikation mehr auf das semantische Verständnis des Zusammenhangs als auf die korrekte Grammatik an. Es genügt also, wenn die Intention des Sprechenden dem Partner in der anderen Sprache vermittelt wird. Dafür gibt es heute schon Demonstratoren: bei der Hotelbuchung zum Beispiel oder für Terminabsprachen. Für den allgemeinen Sprachgebrauch sind die semantischen Hürden noch zu hoch. Wir versuchen jetzt einen neuen Ansatz, der auf «statistischem Lernen» beruht: Wir holen uns grosse Übersetzungsmengen und analysieren, was die «echten» Übersetzer für das Verständnis des Textes herausziehen – und was sie verwerfen. Und das wollen wir in Systemen umsetzen.

Kommen Grossrechner nicht in einen Leistungsbereich, der Maschinen zu Konkurrenten für den Menschen macht? Bleibt der Mensch noch Motor der Innovationsprozesse?
Ohne Zweifel werden Roboter in Zukunft mechanische Routinearbeiten auch im Haushalt übernehmen. Im virtuellen Bereich werden Softwareagenten diese Aufgabe bewältigen. Das reine Faktenwissen dieser Softwareagenten wird zunehmen, aber die Entscheidung, welche Invention man vorantreiben will, was diese Invention in der Gesellschaft bewirken kann, diese Entscheidung wird auch in Zukunft nur der Mensch treffen können.

Das kommt dem Autor so bekannt vor. Wie hatte das jemand vor zwanzig Jahren schon formuliert? «Wir werden zwar eines Tages eine Maschine bauen, die wie ein Hund mit dem Schwanz wackelt, aber keine, die sich dabei freut.» ■

Delano L. Klipstein, dipl. El.-Ing., Fachjournalist, München