HINTERGRUNDPAPIER DER GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

ZUR PRESSEKONFERENZ

"HERAUSFORDERUNG FÜR DIE INFORMATIK:

EMERGENCY COMPUTING UND KRITISCHE INFRASTRUKTUREN"

Die Versorgung unserer Gesellschaft hängt von Computer-Informationsnetzen ab. Technische Defekte, menschliches Versagen oder mutwillige Zerstörungen können gefährliche Kettenreaktionen auslösen. Zuletzt trug der Zusammenbruch der Kommunikationsnetzwerke seinen Teil zur Katastrophe in den vom Hurrikan „Katrina“ verwüsteten amerikanischen Golfstaaten bei. Opfer, Rettungskräfte und Behörden konnten sich untereinander kaum verständigen, weil die zivile Kommunikationsinfrastruktur in weiten Teilen zerstört war.

Emergency Computing

Die Kommunikation ist der Schlüssel für ein effektives Krisenmanagement. Denn Hilfe kann nur dann wirksam sein, wenn Hilfskräfte erfahren können, was wo benötigt wird. Auch können Leib und Leben von Rettungskräften gefährdet sein, wenn ihr Standort unbekannt ist bzw. wenn sie nicht kontaktiert werden können.

Die Informatik verfügt über zahlreiche Forschungspotenziale für innovative Anwendungen, um ein effizientes Katastrophenmanagement zu ermöglichen. Wichtig ist es, die Ablösung veralteter Systeme mit innovativen Lösungen zu betreiben. So können in digitalen Netzen verschiedene Anwendungen implementiert werden. In Objekte eingebaute Sensoren könnten selbständig Aufklärung betreiben, gegebenenfalls Alarm auslösen und notwendige Daten wie etwa Videobilder liefern. Rettungskräfte könnten mit zusätzlichen Informationen in einer „angereicherten Realität“ (augmented reality) unterstützt werden. Damit solche Informationen und Dienste bei der manuellen und häufig gefährlichen Arbeit der Rettungskräfte aber tatsächlich nutzbar sind, müssen speziell angepasste, etwa in die Schutzkleidung und Ausrüstung integrierte IT-Systeme entwickelt werden (wearable computing).

Die Informatik entwickelt außerdem grundlegende Techniken für die Kommunikation unter extremen Bedingungen. So können autonome Kommunikationstechniken, die auf der Stelle, also ad hoc, funktionieren, zusammengebrochene Systeme ersetzen bzw. ergänzen. So genannte Ad-hoc-Netze können dezentral organisiert sein und sich selbst heilen – sollte ein Knotenpunkt ausfallen, muss ein anderer einspringen. Solche Kommunikationsstrukturen können unabhängig vom regulären Stromnetz arbeiten. Einzelne Komponenten können außerdem innerhalb der ad-hoc-Netze direkt

und ohne Umweg miteinander Verbindung aufnehmen. Geräte wie Mobiltelefone, Laptops, Funkgeräte oder Hausantennen, die Daten senden und empfangen können, können in ein solches Kommunikationsnetz integriert werden. Wenn Rettungskräfte aus der ganzen Welt miteinander kommunizieren wollen, müssen die Geräte sofort die selbe Sprache sprechen können und deshalb auch auf offenen Standards aufsetzen. Zudem sollen Unbefugte die Kommunikation nicht stören können. Besonders wichtig ist zudem ein realitätsnahes Training sowie die verlässliche Bewertung der Tauglichkeit von Systemen in komplexen realweltlichen oder simulierten Übungen (virtuelle Realität).

Neben einer Fokussierung auf die Rettungs- und Katastrophendienste müssen Informations- und Meldedienste für den Bürger untersucht werden, welche die neuen mobilen Medien einbeziehen. Damit können Bürger im Katastrophenfall Helfer, Informationslieferanten oder Koordinatoren werden, wenn sie ad hoc in die Kooperationsinfrastrukturen eingebunden werden können.

Angesichts der beschriebenen technischen Potenziale ist die Einsicht entscheidend, dass letztendlich der tatsächliche praktische Einsatz über den Nutzen entscheidet. Daher gehört zu einer verantwortungsvollen Entwicklung in diesen Bereichen die möglichst enge Kooperation mit den Notfallorganisationen, um bedarfsgerechte und gebrauchstaugliche Lösungen erstellen und die optimale Integration in die Arbeitsprozesse realisieren zu können.

Um überzogene Großprojekte zu vermeiden, muss die Verwaltungsinformatikkompetenz des Personals verbessert und das Projektmanagement professionalisiert werden, damit es nicht von der Technik dominiert wird, sondern auch grundlegende organisatorische Probleme angehen kann.

Kritische Infrastrukturen

Die Versorgung mit Energie und Wasser, mit Telekommunikations- und Informationstechnik sowie Mobilität ist für die Gesellschaft lebensnotwendig. Allerdings werden die Versorgungssysteme in den Industriegesellschaften immer komplexer und schwer zu beherrschen. Naturkatastrophen und Terroranschläge, technisches und menschliches Versagen können Kettenreaktionen in weiten Bereichen der Wirtschaft und Gesellschaft auslösen. Zunehmend werden diese so genannten kritischen Infrastrukturen von Computern unterstützt. Dies verstärkt ihre Abhängigkeit von Strom und Informations- und Kommunikationstechnologien.

Nach Auffassung der Gesellschaft für Informatik ist die Voraussetzung für wirksame Beiträge der Informatik-Forschung ein interdisziplinäres Arbeiten, das seitens der Politik unterstützt wird. Die Politik muss dafür Szenarien und Langfristplanungen erstellen und die entsprechenden Forschungsrahmen definieren. Sie muss Sicherheitsbelange institutionell bündeln – problematisch ist hier der Grundkonflikt zwischen Bund und Ländern.

Bundesinnenminister Otto Schily stellte im August eine neue IT-Sicherheitsstrategie als "Nationalen Plan zum Schutz der Informations-Infrastrukturen" (NPSI)[1] vor. Mit dem „Krisenreaktionszentrums IT" im Bundesamt für Sicherheit in der Informationstechnik will Schily ein nationales Lage- und Analysezentrum aufbauen. Es soll jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland verfügen und mit anderen Lage- und Krisenzentren zusammenarbeiten. Außerdem will das Bundesinnenministerium mit den privaten Betreibern von Informationsinfrastrukturen „klare Vereinbarungen" in einem „Umsetzungsplan KRITIS" darüber treffen, wie sie ein effektives Handeln bei IT-Sicherheitsvorfällen sicherstellen können. Der Plan soll Maßnahmen zur Verbesserung der IT-Sicherheitsniveaus festschreiben.

Die Gesellschaft für Informatik begrüßt, dass die Bundesregierung erste Maßnahmen zum Schutz kritischer Informationsinfrastrukturen eingeleitet hat. Allerdings kann die Sicherung kritischer Infrastrukturen nur dann erfolgreich sein, wenn die Anstrengungen nicht nur multidisziplinär, sondern auch transnational sind. Der Forschungsbedarf ist noch erheblich: So müssen die Architekturen der Systeme und Infrastrukturen in einer interdisziplinären Anstrengung von Informatiker/inne/n, Ingenieur/inn/en, Mathematiker/inne/n und Physiker/inne/n verbessert werden. Einzelne Infrastrukturen können zwar robust und widerstandsfähig sein, wenn sie jedoch untereinander vernetzt sind, sind sie es in der Regel nicht. Erstrebenswert sind Systeme, die autark funktionieren und sich selbst überwachen und reparieren können. Auf diese Weise können Dominoeffekte vermieden werden. Zudem müssen Informationen, die in verschiedenen Krisengraden ausgetauscht werden müssen, auch unterschiedlich vertraulich behandelt werden können. Lagezentren müssen bedarfsgerechte Informationen verarbeiten können. Für den Austausch untereinander müssen vertrauenswürdige Systeme entwickelt werden, die über gemeinsame Schnittstellen und Protokolle verbunden sind. Dies bedeutet nicht nur eine wissenschaftliche und technische, sondern auch organisatorische Herausforderung für die Modellierung und Simulation vernetzter Systeme.

Für Rückfragen:
Gesellschaft für Informatik e.V. (GI)
Wissenschaftszentrum, Ahrstr. 45, 53175 Bonn
E-Mail: gs@gi-ev.de, Tel. 0228 / 302 - 145, Fax - 167

1 http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2005/08/Nationaler__Plan__zum__Schutz__der__Informationsinfrastrukturen.html