

ringer sei, je mehr Koppelprodukte (z. B. Stroh) bzw. Rest- und Abfallstoffe in die Energieerzeugung mit einbezogen werden. Einigkeit gab es auch in dem Punkt, das für Baden-Württemberg bestehende bis dato noch nicht ausgeschöpfte Biomassepotenzial für die Erzeugung von biogenen Gasen in jedem Falle nachhaltig zu nutzen. Im Rahmen der Diskussion wurden besonders die Ergebnisse und die Bedeutung der technischen Systemanalyse positiv hervorgehoben.

Wie mehrfach erwähnt, kommt im künftigen Energiesystem der Speicherung von Energie aus Fotovoltaik und Windkraft eine besondere Bedeutung zu. Den Ausführungen zufolge scheint die Bioenergie auf einem guten Wege zu sein, hierzu einen Ausgleich schaffen zu können.

Auch wenn unter den derzeitigen Rahmenbedingungen biogene Gase einem ökonomischen Vergleich zu Erdgas nicht standhalten können, wurde betont, dass für Baden-Württemberg als Innovationsmotor für nachhaltige Mobilität gerade alternative Kraftstoffe und Antriebe eine besondere Relevanz besäßen.

Schuldig blieb die Wissenschaft die Antwort auf die Frage, ob und wie die Technik denn nun in die Praxis kommen könne. Sicherlich ist auch hier die Politik gefragt. So bleibt abzuwarten, wie die aktuelle grün-rote Landesregierung, welche Baden-Württemberg laut Koalitionsvertrag zu den führenden Energie- und Klimaschutzregionen ausbauen möchte, sich diesen Fragestellungen annehmen wird.

### Anmerkung

- 1) Die Vorträge sind unter folgendem Link abrufbar: [https://www.landwirtschaft-bw.info/servlet/PB/menu/1319705\\_11/index.html](https://www.landwirtschaft-bw.info/servlet/PB/menu/1319705_11/index.html).

« »

## Das Internet als superkritische Infrastruktur

Bericht über eine BMBF-Konferenz zum „zukünftigen Internet“

Berlin, 5.–6. Juli 2011

von Arnd Weber, ITAS

Schadprogramme auf dem Internet und Angriffe auf Server bekommen eine größere Bedeutung, wenn das Internet zur Steuerung der Stromversorgung oder zur Verarbeitung medizinischer Daten verwendet wird. Wenn sog. „smart grids“<sup>1</sup> das Internet benutzen, dann hängt die Stromversorgung vom Internet ab und das Internet von der Stromversorgung – das Internet wird so zur „superkritischen Infrastruktur“. Wenn Schadprogramme Arztbriefe verändern, sind die Risiken andere und ggf. größer als beim Zusammenbruch eines Servers oder beim Homebanking. Über neue Nutzungen des Internets und neue Wege aus der Unsicherheit diskutierten mehr als 300 Teilnehmer auf der Konferenz „Zukünftiges Internet“ des Bundesministeriums für Bildung und Forschung (BMBF), die im Berliner Congress Center stattfand.

### 1 Berücksichtigung der Folgen zukünftiger Fördermaßnahmen

Das BMBF hatte neben Vertretern der Wirtschaft und der technischen Forschung erstmals auch Juristen und TA-Forscher gebeten, an der Vorbereitung einer Konferenz mitzuwirken. Ziel des Einbezugs weitere Akteure war, den sozialen Nutzen, den Ressourcenverbrauch und die rechtlichen Anforderungen bei der Entwicklung neuer Verfahren stärker zu berücksichtigen, so der zuständige Abteilungsleiter des BMBF, Wolf-Dieter Lukas. Das ITAS hatte bei der Vorbereitung der Sitzung „Internet als öffentlicher Raum“ mitgearbeitet und Referenten identifiziert. Die Themen dieser Sitzung waren „Öffentlicher Raum und politische Kommunikation“, „Sicherheit, Mobilität und Offenheit“ sowie „Privatheit im Internet“. Die Sitzung wurde vom Leiter des ITAS, Armin Grunwald, moderiert. Daneben fanden weitere

Sitzungen statt zu den Themen „Grenzen und Herausforderungen des Internets“, „kritische Infrastruktur Internet“ und „Suche nach den Metaregeln für die Informationsgesellschaft“ statt. Zusätzlich gab es mehrere Plenarvorträge und eine Podiumsdiskussion.

Aufgrund der Parallelität der Vorträge und der Themenvielfalt soll hier nur über einige Aspekte der zukünftigen Nutzung des Internets berichtet werden, bei denen die potenziellen Risiken besonders deutlich wurden – insbesondere die Sicherheitsrisiken, wie sie in der Stromversorgung, in der Medizin und im motorisierten Verkehr auftreten könnten. Die Diskussion dieser Risiken nahm auf der Tagung breiten Raum ein. Andere Themen, wie die stärkere Nutzung des Internets in der industriellen Fertigung, Netzneutralität (Vorrang oder Behinderung ausgewählter Anwendungen) oder der Energieverbrauch des Netzes werden hier nicht behandelt; zahlreiche der 47 Vorträge sind im Internet verfügbar.<sup>2</sup>

## 2 Sicherheitsprobleme

Die Tagung bot einen breiten Überblick über die Unsicherheit des Internets, d. h. über die Risiken, denen die Endgeräte durch Schadprogramme wie Viren ausgesetzt sind, über die Bedrohungen, die durch abgehörte oder unkorrekt übermittelte Daten entstehen, sowie über die Risiken durch die potenziell mangelnde Verfügbarkeit des Netzes. Diesen Überblick boten v. a. die Plenarvorträge von Michael Hange (Bundesamt für Sicherheit in der Informationstechnik) und Michael (Fraunhofer-Institut für sichere Informationstechnologie).

Bei den Auswirkungen von Schadprogrammen zeigte sich, dass der „Stuxnet“-Angriff einen Schock ausgelöst hatte. Dieses komplexe Programm, das letztlich Maschinensteuerungen von Siemens angreifen sollte, wurde mit mehrjährigem Aufwand und unter Nutzung mehrerer unveröffentlichter Schwachstellen von Microsoft-Programmen erzeugt und verteilt (siehe für Details Falliere 2010). Damit bewies es, dass es Organisationen gibt, die äußerst komplexe Angriffe durchführen. Wenn es solche Organisationen gibt, was heißt das für die Angreifbar-

keit von kritischen Systemen wie Smart Grids oder für die Computer im Gesundheitssystem? Ähnlich gefährlich könnte es werden, wenn die Bremsen eines Autos von einem anderen Auto aus über das Internet ferngesteuert werden. Wenn große Organisationen große Schadprogramme entwickeln, wie kann man sich gegen deren Angriffe schützen? Wer wusste bereits vorher von den Schwachstellen? (Dalton 2009) Sind in IT-Komponenten aus China Hintertüren eingebaut, die Organisationen nutzen können, um Schäden anzurichten?

Hinzu kommt die Frage nach der Verfügbarkeit des Netzes. Was bedeutet es, wenn ein Internetanbieter in China „versehentlich“ auf der ganzen Welt den Datenverkehr umleitet? (Details bei Heise Security 2010) Wenn die Bayer AG über einen längeren Zeitraum Opfer einer Blockade wird („denial of service“, nachlesbar unter RP Online 2011), sind dann nicht noch größere und noch länger andauernde Blockaden zu erwarten? Außerdem: In manchen arabischen Ländern wurde das Internet während der Unruhen am Anfang des Jahres 2011 einfach abgeschaltet. Wie gefährdet ist die Stabilität der Internet-Kommunikation insgesamt? Das Internet hat bislang eine hohe Ausfallsicherheit gezeigt, aber kann man sich darauf verlassen, dass z. B. der größte Internetknoten der Welt in Frankfurt auch zukünftig für andere kritische Infrastrukturen immer verfügbar ist? Wenn der Strom das Internet braucht und umgekehrt das Internet aber Strom, dann wird es zur „superkritischen Infrastruktur“, resümierte Jörg Eberspächer (TU München).

Angesprochen wurde weiter, dass die Angreifbarkeit von PCs noch ein relativ bekanntes und, von „Ausnahmen“ wie eben dargestellt abgesehen, bislang bewältigtes Problem ist. In der Industrie wurde aber beobachtet, dass Smartphones vom Design her unsicherer sind als PCs. Was bedeutet es für Unternehmen, wenn jeder einen derartigen „Spion in der Westentasche“ mit sich herumträgt? (Henning Kagermann, acatech) Wie weit lässt sich die Privatsphäre schützen gegenüber großen, die Daten auswertenden US-Diensteanbietern, vom Cloud Computing bis zu Social Network Services?

### 3 Lösungsansätze

Von Seiten der Wirtschaftsvertreter war zu hören, dass das preiswerte Internet bisher eine hohe Verfügbarkeit hatte und auf dem Markt kein Ersatz in Sicht sei. Trotzdem kam immer wieder die Frage nach einem verbesserten Netz mit höherer Verfügbarkeit und weniger Schadprogrammen auf.<sup>3</sup>

Auf einer anderen Ebene wurde thematisiert, ob der freie Zugang zu Informationen in Ländern mit repressiven Regierungen erleichtert werden könne und ob die Deregulierung des Funkspektrums vorangetrieben werden könne, sodass Komponenten für von Bürgern betriebene Netze, mit entsprechender Reichweite, frei kaufbar wären. Dies würde „rebel nets“ ermöglichen.<sup>4</sup> Außerdem wurde dargestellt, dass für Bürger und Journalisten der freie Zugang zu Informationen wichtig bleibe (Hans Kleinsteuer, Universität Hamburg) und dass die Grenzen der Bürgerbeteiligung noch nicht erreicht seien (Matthias Trénel, Zebralog).

Die frühzeitige Berücksichtigung der Sicherheit beim Bau der Systeme würde Kosten sparen, so Michael Waidner. Hier gäbe es aber ein Problem, weil die Kosten beim Hersteller anfielen, der Nutzen aber bei anderen Parteien. Ohne die frühzeitige Berücksichtigung müsse die Sicherheit im Nachhinein ergänzt oder integriert werden. Man bräuchte eigentlich eine Art „Manhattan project“, so Claire Vishik (Intel), um einer vertrauenswürdigen Infrastruktur näher zu kommen. Komponenten müssten evaluiert und sensible Systeme von anderen isoliert (virtualisiert) werden, um sie so vor Angriffen zu schützen (Dirk Kuhlmann, HP, und Norbert Schirmer, Sirrix). Während die typischen Systeme am Internet mit ausländischen Komponenten umgehen müssen, wurde aber am BMBF-Projekt SEIS (Sicherheit in eingebetteten IP-basierten Systemen) klar, dass es sich für die Automobilindustrie lohnen könnte, sicherheitskritische Daten mit hierzulande entwickelten Komponenten perfekt von Unterhaltungsdaten zu trennen, selbst wenn beide Datentypen über das Internet kommuniziert werden (Daniel Herrscher, BMW).

Der Stuxnet-Angriff hat gezeigt, dass auch Geschäftsgeheimnisse durch Schwächen in den IT-Systemen bedroht sind. Es wurde darauf hingewiesen, dass es keinen vertrauenswürdigen deutschen „global player“ mehr gibt, der hier entgegenwirken könnte. Deutsche Komponenten könnten helfen, vertrauenswürdige Subsysteme zu erstellen. Deren Effektivität bleibt aber vom Funktionieren der Systemumgebungen abhängig. Insgesamt schien man überwältigt von der Innovativität großer US-Firmen, deren neue Produkte hundertmillionenfach gekauft werden, ohne dass transparente Charakteristika oder gar erwiesene Sicherheit gewährleistet würden. Die tatsächlichen Schäden Einzelner sind hier nicht hoch genug, um sofort höhere Ausgaben zu rechtfertigen – die potenziellen Schäden aber ungewiss.

Auf dem Feld des Schutzes der privaten Daten wies Wolf-Dieter Lukas (BMBF) darauf hin, dass Deutschland hier eine wichtige Rolle spiele. Google sei zum Schluss gekommen, wenn ein Dienst mit dem Datenschutz in Deutschland vereinbar sei, dann könne er weltweit verkauft werden. Um Datenschutzregelungen besser durchsetzen zu können, sei es wichtig, sie auf europäischer Ebene, oder besser auf einer noch größeren internationalen Ebene zu harmonisieren (so auch die Vorträge von Marit Hansen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Hannes Federrath, Universität Hamburg, und Wolfgang Hoffmann-Riem, Universität Hamburg). Auch beim Schutz der Privatsphäre sei es wichtig, den Datenschutzen frühzeitig zu berücksichtigen („Privacy by design“) und ihn im Arbeitsleben gelten zu lassen (Annette Mühlberg, Verdi); ähnlich äußerte sich auch Jeroen van der Hoven, der dies aus ethischer Sicht forderte („Value Sensitive Design“).

### 4 Wird die Berücksichtigung sozialer und ökologischer Aspekte zu Erfolgen führen?

Wie Wolf-Dieter Lukas ausführte, soll der Ökonomisierung entgegengewirkt werden, wenn die Sicherheit oder die Umwelt bedroht sind: „Die Ausgestaltung des zukünftigen Internets muss im Rückgriff auf unser Wertesystem den

Menschen als Ausgangspunkt nehmen“ so das Thesenpapier des BMBF (2011). Juristen und Technikfolgenforscher sollen deshalb stärker in die Forschungsförderung einbezogen werden. Offen blieb, wie die Förderung nationaler Projekte und Märkte zu globalen Effekten führen kann.

### Anmerkungen

- 1) Smart grids heißt übersetzt „Intelligente Stromnetze“ und bezeichnet Stromnetze, bei denen Stromverbraucher, Generatoren und Speicher miteinander gekoppelt sind, um Verbrauchsspitzen bzw. Produktionslücken auszugleichen.
- 2) <http://www.future-internet-konferenz.de/>
- 3) Vgl. das BMBF-geförderte „g-lab“ Projekt, das solche Ziele verfolgt; <http://www.german-lab.de/>.
- 4) Vgl. die Vorträge von Robert Horvitz, Open Spectrum Foundation, und zur Deregulierung Arnd Weber, ITAS.

### Literatur

BMBF – Bundesministerium für Bildung und Forschung, 2011: Thesenpapier zum zukünftigen Internet; [http://www.bmbf.de/pubRD/thesen\\_zukuenftiges\\_internet\\_2011.pdf](http://www.bmbf.de/pubRD/thesen_zukuenftiges_internet_2011.pdf) (download 7.11.11)

Dalton, Chr., 2009: A Hypervisor Against Ferrying Away Data. Interview by Franco Furger and Arnd Weber. OpenTC Newsletter April (2009); <http://www.itas.fzk.de/deu/lit/2009/webe09b.htm> (download 7.11.11)

Falliere, N.; O Murchu, L.; Chien, E., 2010: W32. Stuxnet Dossier; <http://www.symantec.com/connect/blogs/w32stuxnet-dossier> (download 7.11.11)

Heise Security, 2010: Chinesischer Provider „entführt“ kurzzeitig Teile des Internets; <http://www.heise.de/security/meldung/Chinesischer-Provider-entfuehrt-kurzzeitig-Teile-des-Internets-975137.html> (download 7.11.11)

RP Online, 2011: Hackerangriff: Bayer hält stand; <http://www.rp-online.de/bergisches-land/leverkusen/nachrichten/hackerangriff-bayer-haelt-stand-1.1322513> (download 7.11.11)

« »

## Die Wissensgesellschaft – angekommen in der Realität?

Bericht von der Konferenz „Von der Informations- zur Wissensgesellschaft: Reloaded“

Prag, 15.–17. Juni 2011

von Lucia Belyová und Gerhard Sardemann,  
ITAS

Bereits 1999 fand in Prag die Konferenz „Von der Informations- zur Wissensgesellschaft. Demokratie – Partizipation – Technikfolgenbeurteilung“ statt, die den Übergang der Gesellschaft in eine Wissens- und Informationsgesellschaft zum Gegenstand hatte. Es sollten wünschenswerte und mögliche Visionen („Technikzukünfte“) im Bereich der Informationsgesellschaft entwickelt werden, wobei weniger deren technische Seite, sondern vielmehr die soziokulturellen Bedingungen und Möglichkeiten einer zukünftigen Gesellschaftsgestaltung ins Blickfeld genommen wurden. Für die diesjährige internationale Konferenz und Jahrestagung des „International Network on Cultural Diversity and New Media“ (CULTMEDIA), die wiederum in Prag stattfand, wurde die damalige Thematik erneut aufgegriffen: „Von der Informations- zur Wissensgesellschaft: Reloaded. e-Partizipation – e-Identity – e-Society“. Dadurch wurde die Möglichkeit eröffnet, zunächst zu prüfen, was von den Überlegungen des Jahres 1999 Bestand hatte, was längst überholt und was neu hinzugekommen ist.

Organisiert wurde die Veranstaltung vom ITAS und vom Zentrum für Wissenschafts-, Technik- und Gesellschaftsstudien am Institut für Philosophie der Akademie der Wissenschaften der Tschechischen Republik. Mit 60 Teilnehmerinnen und Teilnehmern aus sieben europäischen Ländern sowie 24 Vorträgen und Präsentationen stieß sie auf großes Interesse.

Im Sinne der Forschungsschwerpunkte des mit ITAS-Unterstützung im Jahre 2002 gegründeten CULTMEDIA-Netzwerks galt es, aktuelle Entwicklungen im Bereich der Informations- und Kommunikationstechnologien zu diskutieren. Darüber hinaus bestand der Fokus in der Vielfalt und Vielgestaltigkeit darauf bezogener Zu-