Johannes Viehmann

RESEARCH

Das S-Netzwerk und sein wirtschaftliches Potenzial

Die Möglichkeiten des S-Webs und der Jadwirtschaft mit der Einweg-Währung Jad

Springer Vieweg

Das S-Netzwerk und sein wirtschaftliches Potenzial

Johannes Viehmann

Das S-Netzwerk und sein wirtschaftliches Potenzial

Die Möglichkeiten des S-Webs und der Jadwirtschaft mit der Einweg-Währung Jad

Springer Vieweg

Johannes Viehmann
Fraunhofer Institut für Offene
Kommunikationssysteme FOKUS
Berlin, Deutschland

Zugl.: Dissertation, Technische Universität Berlin, 2019

ISBN 978-3-658-28504-3 ISBN 978-3-658-28505-0 (eBook)
https://doi.org/10.1007/978-3-658-28505-0

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Gewidmet

Maria und Paul Steffes

Eugen Viehmann

Vorwort

Im Folgenden werden mit dem S-Netzwerk und der darauf aufbauenden *Jadwirtschaft* zwei einander symbiotisch ergänzende Innovationen vorgestellt. Im Jahr 2004 begann ich, mich mit alternativen Wirtschaftsformen zu beschäftigen. Dabei entstanden bereits die wesentlichen Ideen zur *Jadwirtschaft* als ein System mit offenen Konten und einem nicht beliebig transferierbaren Bezugsmittel. Daraus ergaben sich eine Reihe von Anforderungen, die sich beim bisherigen Stand der Technik und der Forschung nicht realisieren ließen. Aus genau diesen Anforderungen heraus wurde das S-Netzwerk konzipiert – es war ursprünglich explizit als Plattform für den Betrieb der *Jadwirtschaft* gedacht. Erst ab dem Jahr 2007 im Zuge der intensiven Beschäftigung mit rechtsgültig unleugbaren reliablen Publikationen und sicheren Hinterlegungen in einem Informationsnetzwerk im Zusammenspiel mit verlässlicher bidirektionaler semantischer Verlinkung – dem S-Web mit den S-Links – entstand ein Bewusstsein für die universellen Nutzungsmöglichkeiten des S-Netzwerks.

Hier wird entgegen der historischen Entwicklung zuerst das S-Netzwerk vorgestellt, weil das Verständnis in dieser inhaltlich aufbauenden Reihenfolge erleichtert wird. Eine gute Motivation zur Entwicklung des S-Netzwerks lässt sich beispielsweise auch einfach, kurz und naheliegend aus den Anforderungen an eine Plattform für wissenschaftliche Veröffentlichungen aufzeigen – ohne auf die *Jadwirtschaft* eingehen zu müssen.

In dieser interdisziplinären Arbeit werden auch viele weitere technische und wirtschaftliche Anwendungsmöglichkeiten des S-Netzwerks vorgestellt. Am Ende wird mit der *Jadwirtschaft* der ursprünglich Anstoß zur Entwicklung des S-Netzwerks präsentiert. Das S-Netzwerk könnte auch völlig unabhängig von der *Jadwirtschaft* realisiert und genutzt werden. Die beste Wirkung sehe ich jedoch im Zusammenspiel der beiden Innovationen.

Zum Aufbau und Umfang der Dissertation

Mir ist es wichtig, neben einer technischen und ökonomischen Betrachtung hier auch die rechtlichen, sozialen, pädagogischen, psychologischen und ökologischen Aspekte zu beleuchten. Keine einzelne Person kann auf all diesen Gebieten gleichermaßen Experte sein. Ziel konnte es nicht sein, in jede Richtung vergleichbar tief zu gehen. Vielmehr sollen mit der Darstellung in dieser Arbeit Herausforderungen aufgezeigt und Felder für weitere notwendige Forschungsarbeit vorbereitet werden. In diesem vorbereitenden Sinn für künftige Forschungsarbeiten habe ich mich bemüht, dieses Werk so zu gestalten, dass es für Personen aus den verschiedensten Fachgebieten lesbar ist. Es werden daher hier auch einige Grundlagen vermittelt, die für Experten in dem Bereich sicher all-

gemein bekannt sind, die für diesbezügliche Laien aber zum besseren Verständnis sehr hilfreich sein könnten.

Dadurch ergab sich jedoch auch ein allzu großer Umfang. Damit das Ganze handhabbar bleibt, wurden folgende Maßnahmen realisiert: Jedem Kapitel ist eine Zusammenfassung vorangestellt. Details sind in grauen Kästen vom Hauptwerk abgegrenzt. Ferner wurden einige Kapitel in [Viehmann 2018] ausgelagert – sie ergänzen die Dissertation für interessierte Leser zur angestrebten umfassenden Darstellung.

Wissenschaftliche Aussprache, Original und überarbeitete Fassung

Die wissenschaftliche Aussprache vor dem Promotionsausschuss mit dem Vorsitzenden Prof. Dr. Manfred Hauswirth und den Gutachtern Prof. Dr. Ina Schieferdecker, Prof. Dr. Frank Heinemann, Prof. Dr. Gilbert Fridgen und Prof. Dr. Marian Margraf fand am 7. Mai 2019 in Berlin statt. Die Veröffentlichung der von der Fakultät IV – Elektrotechnik und Informatik der Technischen Universität Berlin zur Erlangung des akademischen Grades Doktor der Ingenieurwissenschaften - Dr.-Ing. - genehmigte Originalfassung der Dissertation wurde im klassischen Universitätsdruck vorgenommen. Die Pflichtexemplare wurden an die Universitätsbibliothek der Technischen Universität Berlin übergeben.

Die vorliegende überarbeitete Fassung wurde gegenüber dem Original leicht verändert durch einige kleine Korrekturen und geringfügige Verbesserungen von Abbildungen sowie von Formulierungen bzw. Formatierungen.

Danksagung

Diese Dissertation wurde unterstützt durch meine Betreuer Frau Prof. Dr. Ina Schieferdecker und Herr Prof. Dr. Frank Heinemann sowie durch die Zuwendungen von der Technischen Universität Berlin (Human Centric Communication (H-3C) Graduiertenkolleg) und von dem Fraunhofer Institut für offene Kommunikationssysteme FOKUS in Berlin.

Würdigen möchte ich schließlich die Geduld und das Verständnis für meine Arbeit an diesem Werk in meinem Umfeld, insbesondere von Steffi und Rotraud Viehmann.

Berlin Johannes Viehmann

Inhaltsverzeichnis

Abkürzungen

Allgemein übliche Abkürzungen

API	Application Programming Interface (Programmierschnittstelle)
bzw.	beziehungsweise
bspw.	beispielsweise
Dr.	Doktor
et al.	et alii / aliae / alia (und andere)
etc.	et cetera (und übrige)
evtl.	eventuell
f.	folgende (eine)
ff.	folgende (mehrere)
GB	Gigabyte
ggf.	gegebenenfalls
KB	Kilobyte
MB	Megabyte
ms	Millisekunden
Prof.	Professor(in)
s	Sekunden
S.	Seite
u. a.	unter anderem
z. B.	zum Beispiel

Spezielle Abkürzungen und Symbole in der Dissertation

A	Autorisierer
Σ	Änderungsliste
Γ	Zielpublikum
Δ	Gültigkeitszeitraum
Ξ	Intentionale Interpretation
Π	Herausgeber
T	Publikationszeitpunkt
Λ	Publikationsort
ε	endliche Zeit
Ψ	Threshold (Quorum)
P	Misstrauenspartei / Misstrauensparteien

Jad	Justification, Accounting, Destruction

Abbildungsverzeichnis

Tabellenverzeichnis

1 Die Schaffung des S-Netzwerks aus dem Misstrauen

Das S-Netzwerk ist konzipiert als eine Plattform, die es ihren Teilnehmern erlaubt, reliable Publikationen und sichere Hinterlegungen zu machen und darauf zuzugreifen. Es kombiniert digitale Langzeitarchivierung in einem Computernetzwerk mit Unleugbarkeit und mit weiteren besonderen Gewährleistungen etwa bezüglich der Zugänglichkeit, ohne einzelnen Parteien oder Quoren einfach vertrauen zu müssen. Der Anspruch ist, dass die Rechtsgültigkeit der darin gespeicherten Inhalte und Metadaten mit gleichwertiger Konsequenz für alle Teilnehmer sichergestellt wird.

Zusammen mit dem Konzept der bidirektionalen verlässlichen Verlinkung im S-Netzwerk, dem S-Web, ergeben sich vielfältige neue Möglichkeiten, auf spezialisierte netzwerkseitige Services zu verzichten und so die Risiken alleine auf die Korrektheit und Sicherheit des S-Netzwerks zu reduzieren. Zu den aktuellen Entwicklungstrends Cloud und Web of Services bildet das S-Netzwerk gemeinsam mit dem S-Web einen komplementären Gegenentwurf.

1.1 Einführung

Die Dynamik des Internets verändert die Welt. Darin veröffentlichte Daten unterliegen ebenfalls einer Dynamik – sie sind flüchtig, veränderbar und in vieler Hinsicht unzuverlässig. Das S-Netzwerk soll als relativ statische Ergänzung zum dynamischen Internet mit rechtlichen Garantien sowie sicherheitstechnischen und vertrauensbildenden Maßnahmen digitalen Daten in einem computerbasierten Netzwerk eine für das Informationszeitalter angemessene Tragweite und dauerhaft unleugbare Gültigkeit verleihen.

1.1.1 Ausgangslage – fortschreitende Digitalisierung und Vernetzung

Mit dem Internet existiert ein flexibles weltumspannendes Netzwerk, dessen Entwicklung noch nicht abgeschlossen ist. Derzeit liegen die Grenzen für das Internet nicht nur in der Technik, sondern auch beispielsweise in der Wirtschaft, in der Politik und in der Bildung.

Das Internet, das Netzwerk der Netzwerke [Dennis 2011], ist nicht nur ein robustes Basismedium für digitale Kommunikation aller Art rund um den Globus, sondern es bildet mit den darin verfügbaren Daten auch eine Informationsquelle von zuvor nicht bekannten Dimensionen mit unermesslichen Weiten, Höhen und Tiefen.

J. Viehmann, *Das S-Netzwerk und sein wirtschaftliches Potenzial*,
https://doi.org/10.1007/978-3-658-28505-0_1

Mit dem Internet wird die dynamische Vernetzung von beliebigen Computern, ganzen Computernetzwerken und anderen netzwerkfähigen Geräten wie Mobiltelefonen praktisch überall und jederzeit ermöglicht – in für den Anwender alltagstauglicher Einfachheit.

Grundlage zur Entstehung des Internets (siehe dazu auch [Leiner 1997/2011]) war die Schaffung der Internet Protocol Suite (speziell TCP und IP) durch Robert E. Kahn und Vinton G. Cerf in den 1970er Jahren [Cerf 1974]. Mit der Gründung des Internet Configuration Control Board (ICCB) 1979, dem später das Internet Advisory / Activities / Architecture Board (IAB) folgte [Cerf 1990], und schließlich mit der Gründung der Internet Society ISOC 1992 [Cerf 1992] wurde die Gestaltung des Internets institutional organisiert.

Zunächst diente das Internet primär militärischen und wissenschaftlichen Zwecken. Das NSFNET *Backbone* der *National Science Foundation* in den USA war z. B. zunächst auf Forschung und Bildung beschränkt und durfte erst ab 1992 für kommerzielle sowie private Zwecke genutzt werden, nach einer Gesetzesänderung mit folgender Bedingung:

> *"the Foundation is authorized to foster and support access by the research and education communities to computer networks which may be used substantially for purposes in addition to research and education in the sciences and engineering, if the additional uses will tend to increase the overall capabilities of the networks to support such research and education activities."*, zitiert aus [42USC1862 2007], subsection (g).

Die Bedeutung des noch jungen Mediums Internet entwickelt sich rasant. Laut International Telecommunication Union (ITU) hatte das Internet im Jahr 2000 weltweit 394 Millionen Nutzer, im Jahr 2009 waren es bereits 1.858 Millionen (http://www.itu.int/ict/statistics, 29.12.2011). Trotz dieser Zuwachsraten funktioniert das Internet in der Praxis nach wie vor. Entscheidend für den Erfolg ist, dass das Internet auf offenen Standards aufbaut und dass es flexibel ist. Immer wieder werden neue Anwendungen, Dienstleistungen und Bereiche entdeckt, für die das Internet genutzt werden kann, z. B. *Internet Protocol Television* IPTV [ITU-T 2009] und oder dezentrale Kryptowährungen wie *Bitcoin* [Nakamoto 2008].

Das 1990 von Tim Berners-Lee entwickelte hypertextbasierte Informationssystem World Wide Web hat zusammen mit leicht bedienbaren Webbrowsern entscheidend zur Popularität des Internets beigetragen, da mit der Verlinkung ein einfacher und intuitiver Zugang zu Informationen im Internet ermöglicht wird.

> *"I happened to come along with time, and the right interest and inclination, after hypertext and the Internet had come of age. The task left to me was to marry them"*, zitiert aus [Berners-Lee 1999], S. 7.

> *"The WorldWideWeb browser/editor was working on my machine and Robert's, communicating over the Internet with info.cern.ch server by Christmas Day 1990."*, zitiert aus [Berners-Lee 1999], S. 35.

Obwohl das Internet sich gut bewährt hat, dauert dessen Entwicklung an. Aktuell vollzieht sich der Umstieg auf eine neue Version des Internet Protocols, von IPv4 auf IPv6, der mittlerweile notwendig geworden ist, da der IPv4 Adressraum mit seinen 2^{32} Adressen ausgeschöpft ist [White 2011]. Auch für die Weiterentwicklung des World Wide Webs gibt es Visionen, beispielsweise *"Mind to Mind"* und *"Semantic Web"*:

> *"I have a dream for the web ... and it has two parts.*
> *In the first part, the Web becomes a much more powerful means for collaboration between people. I have always imagined the information space as something to which everyone has immediate and intuitive access, and not just to browse, but to create." ...*
> *"In the second part of the dream, collaboration extend to computers. Machines become capable of analysing all the data on the Web – the content, links and transactions between people and computers. A 'Semantic Web', which should make this possible, has yet to emerge"*, zitiert aus *[Berners-Lee 1999],* S. 169.

Hier soll auch das *"Web of Services"* erwähnt werden, also die Entwicklung von einem Web statischer Daten zu einem Web dynamischer Services [Lemahieu 2001].

Über das Technische hinaus

Das Internet nur technisch zu betrachten, also losgelöst von seiner Umwelt, ist zu reduziert, um dem gesamten Phänomen gerecht werden zu können. Das Internet ist auch ein soziales, ökonomisches, politisches und kulturelles Netzwerk seiner aktiven Teilnehmer.

> *"Each realm of human endeavor continues to create Future Digital Worlds in which represent its things, actions and processes. These digital worlds will be built on the Next Generation computing and communications platform, the Future Internet." ... "The requirements for these digital worlds should drive the design of the Future Internet rather than vice versa." ...*
> *"Perhaps the greatest challenge in envisaging our Future Digital World is to free our minds and overcome our intellectual, technical, and social history to create new visions of the future and to work holistically across current disjoint domains."*, zitiert aus *"The Nature of Our Digital Universe"* [Brodie 2009].

Die *"Seoul Declaration for the Future of the Internet Economy"* der OECD betont die gesellschaftliche Bedeutung der Weiterentwicklung und des Ausbaus des Internets:

> *"The further expansion of the Internet Economy will bolster the free flow of information, freedom of expression, and protection of individual liberties, as critical components of a democratic society and cultural diversity."*, zitiert aus [OECD 2008].

Aktuell sind Limitationen für das Internet gerade auch jenseits der Informationstechnik zu finden. Sie liegen in der Armut und in der oft damit einhergehenden unzureichenden Bildung. Laut Statistik der ITU hatten im Jahr 2009 in den als *"developed"* (Einteilung nach UN M49, http://www.itu.int/ITU-D/ict/definitions/regions/index.html, 7.4.2011) klassifizierten Ländern 61,8% der Haushalte Zugang zum Internet, während in den als *"developing"* eingestuften Ländern nur 13,9% der Haushalte Zugang zum Internet hatten.

Zusätzlich wird das Internet künstlich beschränkt. Zensur führt dazu, dass viele Nutzer nur ein Zerrbild des globalen Internets erreichen können. Die Studien in [Deibert 2008] weisen staatliche Filterungen des Internets in 24 Staaten nach, in denen gegenwärtig über 3,28 Milliarden Menschen leben, wobei insgesamt nur 40 Staaten untersucht wurden. Daneben gibt es auch private Filterungen etwa durch Internet Service Provider und Suchmaschinen-Betreiber. In Deutschland erregten etwa die 2007 zeitweilig vom Provider Arcor gegen einige Porno-Seiten errichteten Sperren Aufsehen, wobei sich kurioserweise ein Anbieter von Sex-Inhalten mit Abmahnungen zur Errichtung von Internetsperren hervortat – offensichtlich zur Bekämpfung der unliebsamen Konkurrenz [Lischka 2007].

Das Internet ist noch so neu, dass die Mehrheit nicht damit aufgewachsen ist. Dies mag einer der Gründe sein, warum das Internet von vielen älteren Personen nicht genutzt wird. So nutzten im ersten Quartal 2010 laut [Destatis 2011] in Deutschland 98 % der 16- und 24-Jährigen das Internet, aber nur 31 % der 65-Jährigen oder Älteren.

Große Teile der Bevölkerung nutzen das Internet nur wenig und wenn dann nur konsumierend, ohne selbst aktiv gestalterisch dazu beizutragen. Laut der Studie „Digitale Gesellschaft" [Wieland 2010] der Initiative D21 sind 35 % der Deutschen „*Digitale Außenseiter*" und weitere 30 % nur Gelegenheitsnutzer. Die Studie stellt auch fest, dass *„viele Millionen Deutsche die neuen Medien nutzen, ohne über ein umfassendes Wissen zum Thema Netz- und Datensicherheit zu verfügen."*, zitiert aus [Wieland 2010]. Im Internet werden standardmäßig oft ressourcenschonende Protokolle ohne Sicherheitsmaßnahmen eingesetzt. Die Nutzer müssen selbst aktiv werden, um etwa mit PGP [Callas 2007] den Inhalt von E-Mails vor fremden Blicken zu schützen. Das erfordert nicht nur Wissen, sondern auch die Bereitschaft, einen zusätzlichen Aufwand zu betreiben.

Vorbehalte und Ängste rund um das Internet sind weit verbreitet. Das Schweizer Bundesamt für Statistik hat eine Umfrage [BFS 2011] zu verschiedenen Bedenken bezüglich des Internets durchgeführt. Der Anteil der Befragten, die sich darin jeweils als *„ehr besorgt“* oder *„sehr besorgt“* bezeichneten, lag bei allen zur Frage stehenden möglichen Gefahren jeweils über 40 %. Besonders hoch war der Anteil der *sehr Besorgten* mit jeweils knapp 30 % beim Thema Kreditkartenmissbrauch und bei der Möglichkeit, dass Kinder mit gefährlichen Personen in Kontakt treten könnten. Jeweils gut 60 % der Befragten zeigten sich *„ehr besorgt“* oder *„sehr besorgt“* bezüglich per E-Mail übertragener Viren sowie bezüglich des möglichen Missbrauchs von privaten Daten.

Speziell was Recht, Vertrauenswürdigkeit und Sicherheit angeht, hat das Internet zumindest einen schlechten Ruf. Laut Bundeskriminalamt [BKA 2010] diente das Internet bei 3,8 % der 2009 in Deutschland (ohne Bayern) erfassten Straftaten als Tatmittel – das sind 206.909 Fälle und mithin 123,6 % der Fälle im Vorjahr 2008. Von allen 2009 erfassten Fällen ist der Anteil der Fälle mit dem Tatmittel Internet bei Betrug mit 19,5 % deutlich höher, bei der Verbreitung von pornografischen Erzeugnissen liegt er gar bei 60,7 % und bei Urheberrechtsverletzungen beträgt er 52,5 %. Die Aufklärungsquote bei Delikten mit dem Tatmittel Internet sank laut Bundeskriminalamt [BKA 2010] zwar von 79,8 % im Jahr 2008 leicht auf 75,7 % im Jahr 2009. Sie liegt damit jedoch immer noch deutlich über der allgemeinen Aufklärungsquote von 55,6 %. Das Internet ist entgegen anderslautenden Gerüchten also weit davon entfernt, ein rechtsfreier Raum zu sein.

Privacy und Authentizität

Die diffuse, sachlich unbegründete Furcht vor einem unkontrollierbaren Internet ohne Recht und Ordnung lässt sich instrumentalisieren, um beispielsweise mehr Überwachung politisch salonfähig zu machen. In Deutschland musste das Bundesverfassungsgericht eingreifen, um eine Gesetzesänderung des Telekommunikationsgesetzes zu kippen, welche eine Vorratsdatenspeicherung in einer so unbeschränkten Form vorsah, dass die im Grundgesetz garantierten Rechte der Bürger dadurch gravierend verletzt wurden [BVerfG 2010].

Es ist angebracht, Staaten und staatliche Institutionen selbst als eine der wichtigsten potenziellen Gefahren im Internet anzusehen. Die *“Global surveillance disclosures 2013”*, in Deutschland als NSA-Affäre bekannt, hat einer breiten Öffentlichkeit vor Augen geführt, wie weit die staatliche Überwachung etwa durch die US-amerikanische *National Security Agency* reicht [Greenwald 2013].

Datenschutz und die Wahrung der Privatsphäre sind für jede Person – auch für jene, welche von sich behaupten, nichts zu verbergen zu haben – von weitreichender Bedeutung:

> *"Perhaps the greatest privacy concern for consumers is that, after they ordered enough products, companies will have accumulated enough personal information to harm or to take advantage of them. With consequences ranging from the threat of junk mail to the denial of health insurance, the problem is serious",* zitiert aus [Berners-Lee 1999], S. 155.

Für gewisse Anwendungen mag auch wieder eine eindeutige starke Authentifikation erforderlich sein, etwa um Geschäfte abschließen zu können.

> *"I believe that the privacy of information I give away is something I ought to have a choice about. People should be able to surf the Web anonymously, or as a well-defined entity, and should be able to control the difference between the two."*, zitiert aus [Berners-Lee 1999], S. 158.

Beides in einem Informationssystem zu vereinen ist nicht einfach und darf als eine der großen Aufgaben für die Netzwerke der Zukunft angesehen werden. Darum und um weitere wichtige Herausforderungen der Vertrauenswürdigkeit, der Sicherheit und der rechtlichen Aspekte von Informationssystemen soll es im Folgenden gehen. Zuerst aber sollen anhand konkreter Anwendungsfälle genau die noch ungelösten Probleme aufgezeigt werden, welche mit der ersten hier präsentierten Innovation – dem S-Netzwerk – direkt angegangen werden sollen.

1.1.2 Offene Probleme als Motivation zur Schaffung des S-Netzwerks

> *Das Internet ist ein unpassendes Medium für wissenschaftliche Veröffentlichungen und andere Informationen, deren unveränderliche sowie unleugbare Verfügbarkeit dauerhaft gewährt bleiben soll und bei denen es darauf ankommt, wer was wann publiziert hat.*

Computernetzwerke können hervorragende und sehr effiziente Informationsquellen sein, da sie ihren Nutzern schnelle Publikationen ermöglichen, auf die andere Teilnehmer mit mächtigen Suchfunktionen bequem von jedem Zugang aus zugreifen können.

Besonders wichtig ist die Vernetzung für die Wissenschaft: Aktuelle Forschungsergebnisse werden beispielsweise oft im Internet zur Verfügung gestellt. Die zeitliche Verzögerung, welche die Herstellung und Distribution von gegenständlichen Medien grundsätzlich mit sich bringt, löst sich dadurch in Luft auf. Für die Recherche sind offene wissenschaftliche Dokumente und Forschungsdaten im Internet auch sehr praktisch, entfällt dadurch doch die Notwendigkeit, mühsam auf Papier gedruckte Zeitschriften, Bücher und andere gegenständliche Medien in Bibliotheken suchen sowie manuell beziehen zu müssen.

Eine Übersicht zu bestehenden Netzwerkplattformen für Wissenschaftler wie Mendeley oder ResearchGATE liefert [Herb 2009]. Zusammenfassend heißt es dort:

„Zum echten Open Access Repository fehlen aber unter anderem Schnittstellen zu Langzeitarchivierungssystemen oder die Vergabe zitierfähiger Identifier."

Problematisch wird es beispielsweise, wenn auf die elektronischen Dokumente in eigenen wissenschaftlichen Arbeiten verweisen werden soll, denn was soll dann als Quelle angegeben werden? Die Internet-Adresse? Diese kann schon am nächsten Tag ungültig sein. Und das passiert tatsächlich auch häufig [Spinellis 2003]. Schlimmer noch: Ein Dokument im Internet, auf das verwiesen wird, kann einfach jederzeit geändert werden. Ein Quellverweis oder ein Zitat ist dann nicht einfach ungültig, sondern unter Umständen völlig falsch – ohne dass zu erkennen wäre, auf welcher Seite nun der Fehler entstanden ist.

Das Internet ist so konzipiert, dass jederzeit im regulären Betrieb einzelne Rechner oder Teilnetzwerke hinzugefügt werden können oder wieder abgetrennt und entfernt werden können – ohne dass das restliche Netzwerk davon berührt oder beeinträchtigt wird. Selbst ungeplante Ausfälle haben in der Regel nur einen sehr begrenzten Schaden zur Folge: Dank der vermaschten Vernetzung können oftmals alle anderen Systeme trotzdem noch über alternative Verbindungen miteinander kommunizieren [Baran 1962]. Aus dem Internet ausscheidende Rechner müssen nicht repariert oder ersetzt werden, damit das Netzwerk weiterhin funktionieren kann. Durch diese Toleranz gegenüber Veränderungen ist das Internet als Kommunikationsmedium sehr robust.

Im Gegensatz dazu können für einzelne Rechner im Internet und erst recht für deren Inhalte keine allgemeingültigen Aussagen zur Verfügbarkeit und zur Ausfallsicherheit gemacht werden, da diese Dinge alleine Sache des jeweiligen Besitzers oder Betreibers sind:

Die dauerhafte Unabänderlichkeit und Erreichbarkeit von einzelnen Adressen, Diensten, Daten oder Seiten werden im Internet prinzipiell nicht garantiert. Ganze Domains können jederzeit aus dem Netz entfernt werden. Adressen können bewusst blockiert oder gezielt umgeleitet werden. Alle Inhalte können ohnehin jederzeit beliebig verändert werden.

Dieser sehr dynamische und mithin flexible Ansatz ist für viele Anwendungen optimal, weil effizient: Nicht mehr benötigte Daten können einfach wieder gelöscht werden. Manche Inhalte sollen auch regelmäßig aktualisiert werden. Die Veränderlichkeit und Flüchtigkeit betrifft im Internet grundsätzlich alle Systeme und Daten. Sie gilt eben auch für Informationen, welche aufgrund ihrer Relevanz eigentlich dauerhaft bewahrt werden müssen und über ein Netzwerk verlässlich verfügbar gemacht werden sollen.

Für die wissenschaftliche Arbeit ist die konzeptionelle Unzuverlässigkeit und Flüchtigkeit von Informationen im Internet ein großes Problem. Auf Informationen aus dem Internet kann kaum zuverlässig verwiesen werden, sie lassen sich nicht einfach als stichhaltiger Beleg verwenden. Falls es neben einer Veröffent-

lichung im Internet auch eine papiergebundene Veröffentlichung in einer Zeitschrift oder einem Buch gibt, besteht natürlich die Möglichkeit, diese als Quelle anzugeben. Wenn man aber nur das elektronische Pendant im Internet gelesen hat, besteht eine gewisse Gefahr, dass diese von der gedruckten Fassung verschieden sein könnte. Muss ohnehin die gegenständliche Version beschafft und gelesen werden, ist der Nutzen einer Veröffentlichung im Internet beschränkt.

Von großer Wichtigkeit gerade in der Wissenschaft ist auch die Feststellbarkeit des genauen Zeitpunkts einer Veröffentlichung. Der Veröffentlichungszeitpunkt ist entscheidend für die Beantwortung der Frage, ob etwas neu ist oder nicht. Rechtsgültig feststellbare Daten zum Publikationszeitpunkt können etwa in patentrechtlichen Fragen entscheidend sein. Eine zuverlässige Zeitangabe, wann etwas ins Internet gelangt, wird jedoch nicht automatisch erfasst. Anders als bei Informationen, die fest an ein gegenständliches Medium wie Papier gebunden sind, lässt sich der Entstehungszeitpunkt von digitalen Daten im Nachhinein auch nicht mehr näherungsweise bestimmen. Für die Wissenschaft muss insbesondere ein Zurückdatieren von Dokumenten unbedingt ausgeschlossen werden.

Interessant ist auch, von wem eine Veröffentlichung gemacht wird. Wer seine Daten ins Internet stellt und nichts weiter unternimmt, der kann sich hinterher nicht mehr als Urheber ausweisen, da andere die Daten kopieren und als ihre eigenen ausgeben können.

Offenbar genügt es für manche Anwendungsgebiete nicht, einfach nur ein Dokument auf irgendeinen Server hochzuladen und es irgendwie in einem Computernetzwerk zugänglich zu machen. Für das wissenschaftliche Arbeiten sind zusätzliche Informationen und Gewährleistungen bezüglich der Zuverlässigkeit sowie der Beständigkeit mehr als nur wünschenswert – sie sind unverzichtbar. Als Medium ist das Internet hier unzureichend.

Diese Problematik betrifft natürlich nicht nur die Forschung und das wissenschaftliche Arbeiten, sondern beispielsweise auch den Journalismus. Im Internet haben sich neue Arten der Berichterstattung etabliert [Briggs 2007]. Die vielleicht wichtigste Konsequenz: Die aktuellen Informationen werden nicht mehr nur von professionellen Journalisten und großen Nachrichten-Konzernen aufgearbeitet und verbreitet, sondern auch von unabhängigen privaten Personen – und zwar potenziell von jedem Nutzer des Internets.

> *„In der Internet-Ära sind wir alle dazu verdammt, Journalisten zu sein.“*, zitiert aus: Peter Glaser, *„Wie Schiffe versenken, nur ernster“*, [Weichert 2010], S. 178.

Meinungsfreiheit erhält mit dem Internet eine neue Dimension. Jeder Nutzer kann selbstständig so publizieren, dass seine Beiträge sofort weltweit verfügbar sind. In zahlreichen Blogs und Foren werden hier wertvolle Beiträge geleistet,

die frei von Konventionen und kommerziellen Zwängen dennoch Millionen zugänglich gemacht werden.

> *„Überall im deutschen Journalismus“ ... „gibt es zwei potenzielle Zensurinstanzen. Die erste Instanz sind die Werbekunden“ ... „mit denen man sich, verständlicherweise, nicht gerne anlegt. Die zweite Instanz sind die Chefredakteure und Verleger“ ...*
> *„Das Internet sorgt nun dafür, dass Meinungen und Meldungen schwerer unterdrückt werden können als früher, es gibt kein Monopol auf öffentliche Äußerungen mehr.“*, zitiert aus *„Mut und Harakiri“* von Harald Martenstein, zu finden in [Weichert 2010], S. 118-119.

Mit dem Internet bieten sich bereits neue technische Möglichkeiten, das Informationsangebot zu bereichern und vom Recht auf freie Meinungsäußerung gebrauch zu machen. Doch manches könnte besser sein: In der Realität werden durch die staatliche Zensur [Deibert 2008] und durch Maßnahmen von Providern sowie Suchmaschinenanbietern auch im Internet erhebliche Schranken errichtet. Außerdem haben die Internetangebote als Informationsquellen erhebliche Mängel gegenüber konventionellen Nachrichtenmedien. Abgesehen von der potenziellen Flüchtigkeit der Daten weiß man in der Regel auch nicht, wer hinter den Meldungen steckt und wann die Veröffentlichung stattfand.

Twitter als Informationsquelle?

Der Kurznachrichtendienst Twitter ermöglicht einen schnellen Austausch von mit Schlagwörtern versehenen kurzen Texten. Wer jedoch wirklich hinter einer Twitter-Meldung steckt, lässt sich für die Leser kaum feststellen. Wie gut der Identitätsklau mit Twitter funktioniert und wie bereitwillig etablierte Nachrichtendienste falsche Meldungen weiterverbreiten, hat beispielsweise eine Aktion des Satiremagazins Titanic bei der Wahl zum deutschen Bundespräsidenten am 30.06.2010 gezeigt:

Sich als Martina Gedeck, Mitglied der Bundesversammlung für die Grünen, ausgebend, wurden falsche Meldungen getwittert. Beispielsweise: *„13:42 Uhr »ok busemann (cdu) hat ne sms bekommen leute :) also kein zweiter wahlgang«.“*, zitiert aus [Wolff 2010].

Verbreitet wurde die Falschmeldung u. a. von ddp, FAZ.net, Bild.de und von der ARD. Dazu mag beigetragen haben, dass bei der vorangegangenen Wahl des Bundespräsidenten am 23. Mai 2009 tatsächlich Abgeordnete schon Ergebnisse getwittert hatten, bevor sie offiziell verkündet wurden [Güßgen 2010].

Mit einer verlässlichen Überprüfbarkeit der Identitäten könnten zumindest Fakes auf Twitter verhindert werden. *„Selbstverständlich ist Twitter in seiner Gesamtheit keine journalistische Quelle. Es wäre ähnlich absurd, darüber zu diskutieren, ob Telefone eine vertrauenswürdige Quelle sind. Sie sind es nicht. Einzelne, verifizierte Anrufer aber sind es und dasselbe gilt für verifizierbare,*

individuelle Twitter-Accounts.“, zitiert aus *„Dem Journalismus geht es erstaunlich gut“* von Wolfgang Blau, zu finden in [Weichert 2010], S. 140.

Abbildung 1: Screenshot vom gefälschten Wendi_Deng Twitter Account

Twitter bietet zwar einen Verifikationsmechanismus. Der Fall um Rupert Murdochs Frau Wendi Deng (siehe Abbildung 1) hat jedoch gezeigt, dass dieser alles andere als vertrauenswürdig ist: Unter dem Namen von Wendi Deng wurde ein gefälschter Twitter Account errichtet und dieser wurde von Twitter als verifiziert markiert [Steier 2012]. Teile der *etablierten* Presse nahmen die falschen Meldungen wiederum dankbar auf [Quinn 2012] und mussten anschließend ihren Irrtum eingestehen [Carroll 2012].

Bei herkömmlichen Zeitungsredaktionen erfahren die Leser die Namen der Verantwortlichen. Außerdem ist stets ein verlässliches Erscheinungsdatum zur Hand. Gedruckte Exemplare lassen sich leicht archivieren und als gegenständliche Belege nutzen. Sie zu fälschen oder zu ändern ist zumindest mit hohem Aufwand verbunden. Unabhängig von der tatsächlichen Seriosität der Inhalte wird durch die Greifbarkeit des Produktes und das rechtliche dafür Einstehen der Produzenten Vertrauen in das Medium an sich geschaffen.

In Zeiten, da Bilder und Filme dank digitaler Technik leicht manipuliert werden können, wären belastbare persönliche Zeugnisse wieder besonders wichtig. Betreibern von Blogs und anderen Nachrichten-Seiten im Internet fehlt die Möglichkeit derartiger Bezeugung.

Auch für Künstler ist es wichtig, sich als Urheber ihrer Schöpfungen auszeichnen zu können. Sie möchten ihre Werke nicht nur dauerhaft erhalten, son-

dern diese auch einem breiten Publikum – auch über ihr Ableben hinaus – verlässlich zugänglich machen können. Eine rechtsgültige Zeitangabe zur Publikation ist für Künstler alleine schon erstrebenswert, um später etwa Plagiatsvorwürfe entkräften zu können.

Das Internet kann den Bedürfnissen von Wissenschaftlern, Journalisten und Künstlern nicht vollauf gerecht werden. Wo hohe Reliabilität von Inhalten gefragt ist, hat es seine Grenzen. Die geforderte Langfristigkeit von Inhalten lässt sich kaum mit jener flexiblen Dynamik vereinen, die das Internet auszeichnet. Wünschenswert wäre eine Plattform, die es erlaubt, Informationen mit gewissen Metadaten und rechtlichen Gewährleistungen unleugbar sowie unabänderlich einem bestimmten Zielpublikum über ein Computernetzwerk dauerhaft zugänglich zu machen. Das S-Netzwerk soll eine solche Plattform werden.

1.1.3 Definitionsbereich

Eine reliable Publikation ist eine rechtsgültige unleugbare und garantiert dauerhaft unabänderlich verfügbare Veröffentlichung. Eine sichere Hinterlegung hat ähnliche Eigenschaften wie eine reliable Publikation, sie darf jedoch nach gewissen Regeln bezüglich ihres Zielpublikums und ihrer Gültigkeitsdauer auch erweitert werden.

Reliable Publikation

Eine Veröffentlichung von Daten χ ist genau dann eine **reliable Publikation** X, wenn gilt:

- Die Publikation X enthält χ und die nachstehenden Zusatzdaten (Metadaten):
  - $\mathbf{\Gamma}_X$ – die Bestimmung des **Zielpublikums**. Γ_X ist eine Gruppe von Personen, die das Rechte haben, auf X lesend zuzugreifen.
  - $\mathbf{\Delta}_X$ – der **Gültigkeitszeitraum** für X. Der Gültigkeitszeitraum Δ_X ist ein geschlossenes Intervall zwischen einem Anfangszeitpunkt und einem Endzeitpunkt.
  - $\mathbf{\Xi}_X$ – die **intentionale Interpretation** von χ. Bei einer digitalen Publikation X wird Ξ_X typischerweise eine Information zum Dateityp von χ sein.
  - $\mathbf{\Pi}_X$ – der **Herausgeber** der Veröffentlichung
  - $\mathbf{T}_X$ – der **Publikationszeitpunkt** von X.
  - $\mathbf{\Lambda}_X$ – der **Publikationsort** von X.

  Es gilt für jede reliable Publikation X: $X = \{ \chi, \Gamma_X, \Delta_X, \Xi_X, \Pi_X, T_X, \Lambda_X \}$. Der Herausgeber kann die Werte für Γ_X und Ξ_X frei wählen. Der Gültigkeitszeitraum Δ_X ist auch weitgehend frei wählbar, er darf nur nicht vor dem Publika-

tionszeitpunkt T_X beginnen. Die Werte für Π_X, T_X und Λ_X sind Messwerte, die verifiziert werden müssen.

- Auf die Veröffentlichung X muss mit einem konstanten universellen und einmaligen **Identifikationsmerkmal I_X** eineindeutig verwiesen werden können.
- Für den kompletten Gültigkeitszeitraum Δ_X muss jede Person aus dem vorab festgelegten Zielpublikum Γ_X anhand des Identifikationsmerkmals I_X in **endlicher Zeit ε_X** lesenden Zugriff auf die unveränderte Publikation X erhalten.
- Die rechtlichen Konsequenzen, welche das Publizieren von X hat, müssen exakt spezifiziert sein. Die Zusatzdaten sind rechtlich bindende Angaben. Die Daten χ haben in ihrer intentionalen Interpretation Ξ_X Rechtsgültigkeit.

Das Zielpublikum Γ_X kann eine abzählbar unbegrenzte Menge von Personen sein. Das Ende des Gültigkeitszeitraums Δ_X darf offen sein. Die nicht zu den Metadaten von X gehörende Zeit ε_X, in der jede Person aus dem Zielpublikum Γ_X während des Gültigkeitszeitraums Δ_X lesenden Zugriff auf die Publikation X zu erhalten hat, kann durch eine Konstante bestimmt sein oder durch eine Funktion etwa abhängig von der Größe der Daten χ berechnet werden.

Niemand, auch nicht der Herausgeber Π_X selbst, darf eine reliable Publikation X bis zum Ende des Gültigkeitszeitraums Δ_X auch nur irgendwie verändern können. Jede reliable Publikation muss strikt unleugbar (*non-repudiation*) sein.

Sichere Hinterlegung

Eine **sichere Hinterlegung** X von Daten χ ist ähnlich wie eine reliable Publikation. Bei sicheren Hinterlegungen ist es jedoch auch möglich, nachträglich weiteren Personen Leserechte einzuräumen und den Gültigkeitszeitraum zu erweitern. Wem jedoch einmal Leserechte eingeräumt sind, dem dürfen diese Rechte nicht nachträglich wieder entzogen werden – eine sichere Hinterlegung ist unleugbar und Erweiterungen sind zu protokollieren.

Eine Deposition von Daten χ ist genau dann eine **sichere Hinterlegung** X, wenn gilt:

- Eine sicherer Hinterlegung X von Daten χ beinhaltet χ sowie die Metadaten Γ_X, Δ_X, Ξ_X, Π_X, T_X und Λ_X wie bei einer reliablen Publikation und zusätzlich folgende Metadaten:
  - $\mathbf{A}_X$ – die **Autorisierer**. Das Zielpublikum Γ_X und der Gültigkeitszeitraum Δ_X können nachträglich ausschließlich von Personen aus A_X erweitert werden. Die Verlegung des Endzeitpunkts weiter in die Zukunft ist die einzige zulässige Änderung von Δ_X. Autorisierer dürfen außerdem auch zu A_X Personen hinzufügen.

- Σ_X – die **Änderungsliste**. Für alle Leseberechtigten Γ_X muss, solange sie auf *X* zugreifen dürfen, feststellbar sein, wann wer Leserechte von wem erhalten hat und wer wann den Gültigkeitszeitraum Δ_X wie erweitert hat. Auch muss nachvollziehbar sein, wer ab wann zu den Autorisierern A_X gehört. Änderungen von A_X, Γ_X und von Δ_X müssen dazu in Σ_X mit Zeitangaben unleugbar protokolliert werden.
  Die Änderungsliste Σ_X darf nur zu diesem Zweck erweitert werden, von Personen, welche zum jeweiligen Zeitpunkt zur Menge der Autorisierer A_X gehören.

Es gilt folglich für eine jede sichere Hinterlegung *X*:

$X = \{ \chi, A_X, \Sigma_X, \Gamma_X, \Delta_X, \Xi_X, \Pi_X, T_X, \Lambda_X \}$.

- Bei sicheren Hinterlegungen kann jede Person *P* einen eigenen persönlichen **Zugriffszeitraum Δ_{PX}** haben, der frühestens zu dem Zeitpunkt beginnt, zu dem eine Person *P* zum Zielpublikum Γ_X hinzugefügt wird. Der persönliche Zugriffszeitraum kann in der Änderungsliste Σ_X explizit angegeben werden. Er muss innerhalb des Gültigkeitszeitraums Δ_X liegen und kann nur erweitert werden.
- Ansonsten gelten Entsprechungen zu sämtlichen Eigenschaften reliabler Publikationen.

Zur Verwendung des Begriffs der Reliablen Publikation

> *„Il n'a plus de nom. Et toi non plus, tu n'as plus de nom, cramponné à la barre. Il n'y a plus que le bateau qui ait un nom et la tempête. Est-ce que tu le comprends?*
> *ANTIGONE (secoue la tête): Je ne veux pas comprendre. C'est bon pour vous. Moi, je suis là pour autre chose que pour comprendre. Je suis là pour vous dire non et pour mourir.“*, zitiert aus [Anouilh 2001], S. 55.

Eigene Übersetzung:
„Er hat keinen Namen mehr. Und du, du hast auch keinen Namen mehr, klammerst dich an das Ruder. Es gibt nichts mehr außer dem Boot, das einen Namen hat – und den Sturm. Verstehst du das?
ANTIGONE (schüttelt den Kopf): Ich will nicht verstehen. Verstehen, das ist gut für Euch. Ich bin für etwas anderes da, als um etwas zu verstehen. Ich bin da um Euch nein zu sagen und um zu sterben.“

So wie Kreon an Antigone vorbeiredet und wie Antigone nicht verstehen will, ist die Katastrophe in dem Drama unabwendbar. Autoren haben es wohl leichter als Kreon: Freiwillige Leser ihrer Werke haben zumindest initial bestimmt ein Interesse, auch zu verstehen. Und doch kommt es zu Verständnisproblemen, trotz des Bestrebens der Autoren, verstanden zu werden sowie des Willens der Leser zu begreifen. Wo Alltagssprache die nötige Präzision

fehlt, kann wissenschaftliche Sprache ermüdend sein. Es sollte versucht werden, möglichst wenig neu zu definieren.

Um diese Dissertation schreiben zu können, wäre es auch möglich, sich mit der Definition der *sicheren Hinterlegung* zu begnügen, denn eine *reliable Publikation* ist de facto eine spezielle Form der *sicheren Hinterlegung*, eben mit leerer Menge der Autorisierer A_X. Hier wird trotzdem der Begriff der *reliablen Publikation* eingeführt, weil dieser einfacher zu erklären und zu verstehen ist. Eine Plattform ausschließlich für *reliable Publikationen* ließe sich leichter implementieren. *Reliable Publikationen* lassen sich effizienter handhaben – zur Feststellung, ob jemand zugriffsberechtigt ist, müssen keine Änderungen in Σ_X auf Zulässigkeit geprüft und ausgewertet werden.

Die Verwendung beider Begriffe im Zusammenhang mit dem S-Netzwerk soll nicht zuletzt auch die damit einhergehenden verschiedenen primären Verwendungsmöglichkeiten (Veröffentlichung, Deposition) verdeutlichen. So wird im Folgenden, je nachdem, ob nachträgliche Erweiterungen überflüssig oder erforderlich sind, nur der Begriff der *reliablen Publikation* oder nur der Begriff der *sicheren Hinterlegung* verwendet. Sonst werden beide Bezeichnungen aufgeführt.

1.1.4 Idee und Zielsetzung für das S-Netzwerk

Das S-Netzwerk soll für einmal darin gespeicherte Informationen die Eigenschaften von reliablen Publikationen beziehungsweise von sicheren Hinterlegungen garantieren können. Jeder Teilnehmer soll in einer endlichen Durchführungszeit selbst reliablen Publikationen und sichere Hinterlegungen im S-Netzwerk machen können.

Das S-Netzwerk soll ein hochgradig vertrauenswürdiges Medium für unleugbare Daten werden, welches aus einem informationstechnischen System in Kombination mit einer rechtlichen Basis besteht. Es soll seinen Nutzern ermöglichen, rein informationsbasiert reliable Publikationen und sichere Hinterlegungen in einem Computernetzwerk zu machen sowie darauf zuzugreifen. Es soll als Plattform für jene digitalen Daten dienen, welche besonderer rechtsgültiger Gewährleistungen bezüglich ihrer Verfügbarkeit, Dauerhaftigkeit und Korrektheit bedürfen.

Gedacht ist das S-Netzwerk als internationales, idealerweise global nutzbares Medium. Für die rechtliche Tragweite und Konsequenz von Publikationen sowie Hinterlegungen im S-Netzwerk sollen netzweit für alle Teilnehmer möglichst gleichwertige Standards gelten. Am S-Netzwerk sollen nur natürliche oder juristische Personen partizipieren dürfen, welche die Regeln des S-Netzwerks rechtsverbindlich akzeptieren und respektieren.

Die Eigenschaften von reliablen Publikationen und sicheren Hinterlegungen soll das S-Netzwerk langfristig gewährleisten, auch mit großen Teilnehmerzahlen.