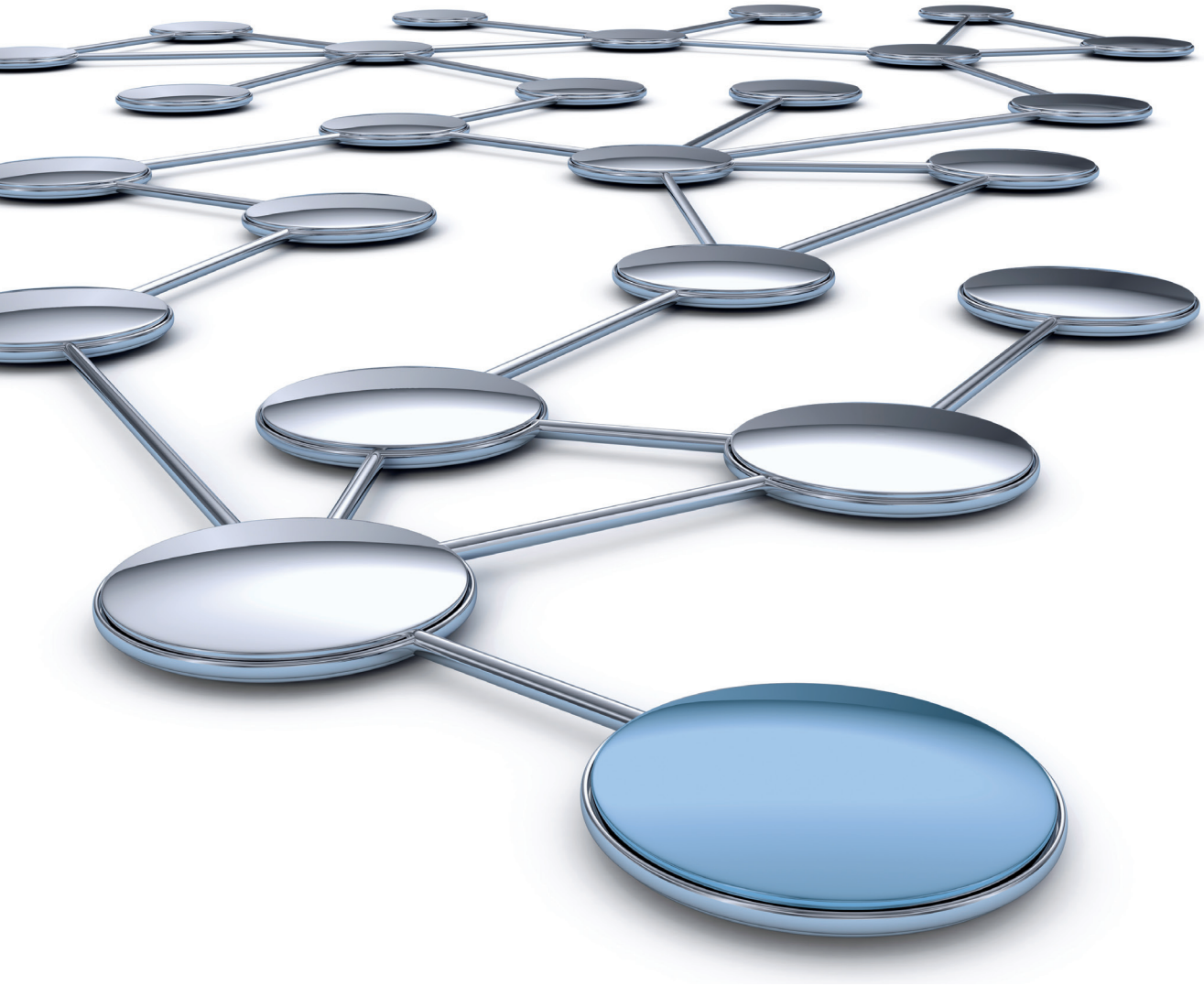
Technologietrends



OSINT

Report 2/2010

ISN ETH Zurich

INTERNATIONAL RELATIONS AND SECURITY NETWORK

ETH Zurich | Leonhardshalde 21, LEH | 8092 Zurich | Switzerland
Tel: +41 (0)44 632 04 24 | Fax: +41 (0)44 632 14 13
www.isn.ethz.ch | osint@sipo.gess.ethz.ch

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Authors: Felix Juhl, Florian Schaurer, Jan Störger

International Relations and Security Network (ISN)
ETH Zurich
Leonhardshalde 21, LEH
8092 Zurich
Switzerland
Tel.: +41 (0)44 632 04 24

osint@sipo.gess.ethz.ch
www.isn.ethz.ch

Project supervision: Andreas Wenger, Director CSS; Victor Mauer, Deputy Director CSS

Themenübersicht

OSINT Report 2/2010

Technologietrends

Cloud Computing

Cloud Computing oder *the Cloud – die Wolke* wird von der Industrie und den Medien als die grösste Revolution der Informationstechnologie gefeiert. Unternehmen müssen für den Umstieg auf dieses neuartige Betriebsmodell ihre vorhandenen Anwendungen nicht anpassen oder gar austauschen, so die IT Branche, sondern können diese ohne grosse Umstände auf Cloud-Computing-Plattformen migrieren.

Dem Trend entsprechend etablieren sich immer mehr Unternehmen aus diversen Bereichen als Cloud-Service- und Infrastruktur-Anbieter und bieten entsprechende Plattformen und Leistungen an. Prominente Beispiele wie Google, das sich vom Suchanbieter längst zum cloud-basierten Online-Service-Riesen entwickelt hat, oder Amazon, das neben Shopping inzwischen auch Services bietet wie die Elastic Compute Cloud (EC2), mit Facebook als bekanntestem Kunden oder der Simple Storage Service (S3) lassen erkennen, in welche Richtung sich Massendatenverarbeitung und -speicherung entwickeln.

Obwohl eine einheitliche Definition fehlt, gibt es einen grundsätzlichen Konsens, welche Elemente Cloud Computing umfasst. Die zentralen Eigenschaften sind Infrastrukturservices (Datenbank, Datenspeicher, Rechenleistung) und Applikationsservices (E-Mail, Customer Relationship Management CRM).Diese können über Standard-Internetprotokolle orts- bzw. geräteunabhängig genutzt werden. Das besondere hierbei sind intelligente Automatisierungen, die bei Bedarf mehr Speicher oder Rechenleistung spontan zur Verfügung stellen, ohne eine Interaktion des Nutzers.

Cloud Services sind hochverfügbar, skalierbar und lassen sich *on Demand*, also auf Abruf, nutzen. Cloud-Computing-Plattformen bieten Applikationsschnittstellen und können so nutzerspezifisch genutzt und erweitert werden, ohne dass der Nutzer dabei selbst in die Bereitstellung von Infrastruktur, deren Wartung oder Sicherheit investieren muss.

Was für eine Revolution gehalten wird, ist objektiv betrachtet kein Produkt, das über Nacht entstanden ist, sondern das Resultat verschiedener längerfristiger technologischer Trends. Cloud Computing ist also vielmehr ein Überbegriff, der ein System von Webtechnologien, Architekturen, Serviceangeboten sowie Businessmodellen und Automatisierungen beschreibt.

Die Entwicklung dieses Technologiekonzepts ist vergleichbar mit dem Übergang zur zentralisierten flächendeckenden Stromversorgung Anfang des 20. Jahrhunderts. War es zu Beginn der Industrialisierung üblich, Strom dort zu erzeugen, wo der Bedarf entstand, begannen sich nun ausgedehnte Stromnetze über das ganze Land zu erstrecken, gespeist von wenigen zentralen Grosskraftwerken. Ähnlich wie Strom wird der Verbrauch abgerechnet, nur eben nicht pro Kilowattstunde, sondern in Gigabyte.

Der Weg der Fortentwicklung vom Internet als reine Ansammlung von Inhalten hin zur Cloud begann um die Jahrtausendwende, als Technologiefirmen das Konzept vom *semantischen Web* entwickelten. Zugrunde liegt die Idee, das Internet nicht nur Anwendern und ihren Webbrowsern nutzbar zu machen, sondern es für Applikationen

NOTIZEN

und Programmierer zu öffnen. Während das World Wide Web eine Möglichkeit darstellt, alle Daten der Welt miteinander zu vernetzen, zeigt das semantische Web einen Weg auf, um die Informationen der Welt auf der Ebene ihrer Bedeutung miteinander zu verknüpfen, also die Bedeutung von Informationen für Computer, nicht nur für Menschen, verwertbar zu machen.

71 Prozent der sogenannten IT-Entscheider weltweit sind sich einig, so lautet das Ergebnis einer weltweiten Studie der US-Beratungsgesellschaft Avanade Inc., Cloud Computing sei eine Technologie-Chance, die helfe, sich auf das Kerngeschäft zu konzentrieren, schneller auf Veränderungen zu reagieren und damit die eigene Flexibilität zu steigern.

In der Schweiz reagierten, laut dieser Studie, Budgetverantwortliche weitaus zurückhaltender und differenzierter. Für 70 Prozent ist Cloud Computing nicht viel mehr als eine Modeerscheinung auch wenn der Nutzen, den Cloud Computing mit sich bringt, erkannt wird. Immerhin sind 40 Prozent der Meinung, dass sich mit der jungen Technologie durchaus die IT-Einstiegskosten reduzieren liessen. Eine ausserordentliche Mehrheit von 90 Prozent der in der Studie befragten Schweizer Verantwortlichen allerdings vertraut ihren bestehenden internen Systemen mehr als Lösungen aus bzw. in der Cloud. Sicherheitsbedenken und die Skepsis, die Kontrolle über eigene Daten und Systeme aus der Hand zu geben, überwiegen und relativieren beworbene Vorteile.

Der Grund für die Zurückhaltung ist begründet. Cloud Computing hat nicht nur Vorteile, sondern birgt auch Risiken und offene Fragen. Tatsächlich gilt es, eine Vielzahl von Sicherheitsaspekten zu beachten. Sind z.B. Daten und Informationen erst einmal in der Wolke, ist es nicht leicht, diese wieder zurückzuholen, oder gar zu löschen. Weitgehend ohne Einflussnahme des Nutzers findet eine Informations- und Lastverteilung von Daten und Informationen über Ländergrenzen hinweg statt. Diese unterliegen dann unter Umständen anderen, unbekannten lokalen Gesetzen oder Verordnungen.

Aus dieser entfernten und schwer kontrollierbaren Nutzung und Speicherung ergeben sich teils erhebliche datenschutzrechtliche Probleme. Aus Sicht der Daten- und Informationssicherheit ist anzuraten, die Problematik der rechtlichen und regulatorischen Erfordernisse sowie der für sie anwendbaren Rechtsordnungen im Sinne von Datenschutz und Verfügbarkeit kritisch zu prüfen. Denn wer die Daten wo verarbeitet, ob sie dort wirklich sicher sind und wer auf sie Zugriff hat, weiss oft niemand und Sicherheitsgarantien bekommt man selten.

Aufgrund der verteilten Rechner- und Speicherleistung, die der Kunde als Cloud Services erwirbt, bestehen im Allgemeinen keine Möglichkeiten, Zugriffskontrollen und rollenbasiertes Rechtemanagement (bzw. Mandantentrennung) durchgängig sicherzustellen. Zu beachten ist insbesondere auch, dass nach Beendigung des Auftrags die verarbeiteten Daten und alle Zwischenergebnisse in der Cloud gelöscht werden müssen. Hier ist überhaupt nicht klar, wie dies technisch gewährleistet werden kann.

Ein weiterer, oft unbedachter Risikofaktor ist der Handel mit Storagekapazitäten. Sollte sich Cloud Computing ähnlich dem Strommarkt entwickeln, dann werden Provider von Cloud Computing voraussichtlich einen Handel über eine *Ressourcenbörse* untereinander aufbauen. Auf dieser Börse werden Ressourcen zu einem bestimmten Preis angeboten. In Leistungsspitzen würde sich zum Beispiel der Preis für Prozessorleistung pro Stunde erhöhen und auf der Börse entsprechend gehandelt werden. Welche Konsequenzen dies für die Sicherheit der Daten hat, ist noch vollkommen unklar.

Die Gefahr von Manipulation, Diebstahl oder Spionage wird im Zusammenhang mit Cloud Computing erstaunlicherweise kaum erwähnt. Solide technische Massnahmen zur Absicherung von Cloud Services sind wichtig und bereits heute einsetzbar. Noch wichtiger jedoch ist die Ausgestaltung der Beziehung zum Cloud-Dienstleister und der damit verknüpften Aktivitäten, die den Rahmen für die technologische Zusammenarbeit prägen. Risikoanalysen, Service Level Agreements und Provider-Management sind mit Blick auf Cloud Security der Schlüssel zum Erfolg.

Social Tagging

Social Tagging bezeichnet die anwenderseitige, kollaborative Indexierung und Klassifizierung von Information und die damit einhergehende Herstellung von Laien-Taxonomien, sogenannten *Folksonomies*. Mithilfe entsprechender Anwendungen und Dienste, so vor allem Plattformen zum Sammeln und Austauschen sozialer Lesezeichen, Register und Kataloge, werden digitale

NOTIZEN

Inhalte (Texte, Bilder, Videos, Musik etc.) lexikalisch und semantisch verschlagwortet, sachlich erschlossen, verwaltet, bewertet und kommentiert, visualisiert (etwa in *tag clouds*), anderen Nutzern verfügbar gemacht und bilden damit eine Form der Wissensrepräsentation auf der Basis kollektiver Intelligenz. Diese wiederum basiert auf dem Phänomen der Emergenz, also auf der Annahme, dass soziale Organismen mehr Intelligenz hervorbringen als die blosse Summe ihrer autonomen Teile.

Gerade für die zentralisierte Sammlung, dynamische Bereitstellung und interaktive Aufarbeitung von spezifischen Wissensressourcen innerhalb von Organisationen eignen sich daher entsprechende Instrumente. Zu beachten ist, dass im Gegensatz zu den weitverbreiteten, allgemein zugänglichen, mitunter anonymisierten und nur lose moderierten Social Tagging-Diensten im Internet die Steuerung abgeschlossener bzw. intern offener Benutzerkreise trotz geringerer Teilnehmerzahl (und damit potentiell geringerer kollektiver Intelligenz) wertvolle Kontrollmöglichkeiten des Quellenaufbaus bietet. Allen voran ist hier die Standardisierung der verwendeten Taxonomie und damit die Präzisierung der Beschlagwortung, letztlich die Erhöhung des Nutzens informationeller Kontextualisierung an sich zu nennen. Während bei völlig freier Indexierung mangelnde Konsistenz der Einordnung eher Regel als Ausnahme ist (so kann ein Buch unter „Buch“, „Bücher“, „Literatur“, „Roman“ oder „Propaganda“ usw. zu finden sein), lassen sich intern eindeutige Kategorien vorgeben.

Die vom ISN erarbeitete und ständig aktualisierte Taxonomie ist ein umfangreiches Beispiel für die Verständigung auf einheitliche Zuordnung und reproduzierbare Wissensorganisation. Es erweist sich hier als Mindestanforderung, Information nach a) Art der Quelle, b) geographischem sowie c) inhaltlichem, thematischen oder personellen Bezug zu erschliessen, wobei vom Allgemeinen hin zum Speziellen klassifiziert wird. Die manuelle Zusammenfassung, Kommentierung und Bewertung der Quelle bietet schliesslich den eigentlichen analytischen Mehrwert und setzt neben andauernder formaler wie inhaltlicher Pflege des Archivs die klare Kommunikation über Fragestellung und Beschaffungsziele voraus.

Konzeptionelle und praktische Herausforderungen

Open Source Intelligence – Modellierung

In der Diskussion um die Bedeutung von Open Source Intelligence für Nachrichtendienste und einer möglichen Rolle von nichtstaatlichen Akteuren hierbei scheint es geboten, durch Definitionen und Annahmen für Klarheit zu sorgen und ausgehend davon möglicherweise Erkenntnisse abzuleiten, die für die Gewährleistung staatlicher Sicherheit relevant sind.

Der Begriff Intelligence wird im Folgenden als Dienstleistung von Nachrichtendiensten verstanden. Sofern er nicht explizit in einen anderen, bspw. privatwirtschaftlichen Zusammenhang gestellt wird, ist ein staatlicher Kontext und ein entsprechendes Mandat vorausgesetzt. Desweiteren gilt hier die Annahme, dass Nachrichtendienste in erster Linie erweiterte rechtliche Befugnisse gegenüber der Öffentlichkeit, nicht aber zwangsläufig mehr Fähigkeiten oder Ressourcen als diese haben. Ferner wird davon ausgegangen, dass Nachrichtendienste diese erweiterten rechtlichen Befugnisse jedoch nicht überschreiten.

Als Ausgangspunkt einer wissenschaftlichen Betrachtung nachrichtendienstlicher Leistung, bzw. des weit über den englischsprachigen Raum hinaus verbreiteten Begriffs Intelligence, erscheint eine Definition derselben sinnvoll. Hier wird im Weiteren Intelligence als die Sammlung, Verarbeitung, Analyse, Produktion, Validierung, Klassifizierung und Verteilung von Information sowie deren Schutz in staatlichem Auftrag verstanden. Dies macht deutlich, dass es sich stets um eine Dienstleistung für den Staat handeln, diese aber nicht zwangsläufig auch von diesem erbracht werden muss. Hieraus ergibt sich also grundsätzlich die Möglichkeit nichtbehördlicher *Nachrichtendienstleistungen* (NDL), deren Auftraggeber und Abnehmer jedoch nach wie vor der Staat sein muss. Den Staat hier unter anderem als Abnehmer zu bezeichnen, schliesst auch eine Leistungskontrolle durch den Auftraggeber mit ein. Dies dürfte insbesondere, jedoch keinesfalls ausschliesslich, für die Zusammenarbeit mit nicht-staatlichen Dienstleistern von Bedeutung sein. Die hier implizierten Dienstleistungen beziehen sich ausschliesslich auf den rein informationellen Bedarf der bezugsberechtigten Stellen.

NOTIZEN

Bei der Vielzahl von sogenannten nachrichtendienstlichen Disziplinen wie bspw. HUMINT, SIGINT oder OSINT fehlt es bisher an einer systematischen Unterscheidung, die in den hier relevanten Zusammenhängen zudem wesentlich vereinfacht werden kann. So werden nachrichtendienstliche Quellen und Mittel einerseits nach deren Art und andererseits nach deren Zugänglichkeit unterschieden. Dabei gibt es einzig die Typen Human Intelligence (HUMINT), unter Verwendung menschlicher Quellen und Mittel, und Technological Intelligence (TECHINT), unter Verwendung technologischer Quellen und Mittel. Bezüglich der Zugänglichkeit wird lediglich zwischen Open Source Intelligence (OSINT), unter Verwendung offen, also für die Öffentlichkeit legal und tatsächlich zugänglicher Quellen und Mittel, und *Non-Open Source Intelligence* (NOSINT), unter Verwendung nicht offen zugänglicher Quellen und Mittel, unterschieden. Freilich sind diese beiden Begriffe intrinsisch irreführend, da sie zunächst nur auf die Zugänglichkeit der Quellen und nicht der Mittel hinweisen. Hier wird jedoch davon ausgegangen, dass OSINT implizit nicht nur die offene Zugänglichkeit ihrer Quellen, sondern auch ihrer Mittel erfordert. Ausserdem setzt, wie oben bereits angenommen, eine offene Zugänglichkeit die legale und tatsächliche Zugänglichkeit der Quellen und Mittel durch die Öffentlichkeit voraus. So wird ausgeschlossen, dass OSINT unter Verwendung zwar tatsächlich, nicht aber legal zugänglicher Quellen und Mittel erbracht werden kann (bspw. Hacking). Bemerkenswert ist in jedem Fall, dass durch die zweifache Unterscheidung nachrichtendienstlicher Disziplinen nach Art und Zugänglichkeit der Quellen und Mittel HUMINT und TECHNIT sowohl jeweils OSINT als auch NOSINT sein können.

Es erscheint letztlich trivial, dass eine Nachrichtendienstleistung stets, unter Wahrung der rechtlichen Befugnisse des Erbringers, alle Informationen sowie die entsprechenden Quellen und Mittel, die für den staatlichen Auftrag potentiell relevant sind, einbeziehen sollte. Somit ist eine Konzentration auf die eine oder andere nachrichtendienstliche Disziplin, ohne auftrags- und umstandsorientierte Begründung nicht zu rechtfertigen. Sofern also für einen staatlichen Auftrag relevante Information durch OSINT gewonnen werden kann, muss diese in der gesamten NDL angemessene Berücksichtigung finden, um einen Informationsnachteil gegenüber der Öffentlichkeit, und nicht zuletzt auch feindlicher Kräfte, zu vermeiden.

Es erscheint geboten, innerhalb der Öffentlichkeit zwischen einer allgemeinen und einer spezialisierten Teilöffentlichkeit zu unterscheiden. Letztere unterscheidet sich von ersterer in einer möglichen Exklusivität, was die Fähigkeiten einzelner Mitglieder angeht. Während davon ausgegangen wird, dass jedermann gleichermassen der allgemeinen Öffentlichkeit angehört, ist trotz gleicher rechtlicher Befugnisse nicht jeder auch im gleichen Masse und in gleicher Weise befähigt, spezialisiert oder hat Zugang zu speziellen Quellen und Mitteln. Dies erlaubt Fälle zu betrachten, in denen zwar nicht die allgemeine Öffentlichkeit, doch aber die spezialisierte Öffentlichkeit nachrichtendienstliche Quellen, Mittel oder gar Leistungen bereitstellen kann.

Somit ergeben sich die Unterscheidungen zwischen allgemeiner und spezialisierter Öffentlichkeit hinsichtlich deren Fähigkeiten einerseits, sowie zwischen der Öffentlichkeit insgesamt und den Nachrichtendiensten hinsichtlich deren rechtlicher Befugnisse andererseits.

Aus der Unterscheidung zwischen Quellen und Mitteln einerseits und deren jeweiliger tatsächlicher und legaler Zugänglichkeit andererseits ergeben sich theoretisch 2^4, also 16 Fälle, wovon nur ein einziger die allgemeine Öffentlichkeit zulässt und nur drei Fälle die spezialisierte Öffentlichkeit miteinschliessen. Die spezialisierte Öffentlichkeit mag spezielle, technische (TECHINT) oder menschliche (HUMINT), jedoch legale Quellen und Mittel (OSINT) zur Verfügung haben, sobald aber Quellen oder Mittel nur innerhalb entsprechender erweiterter rechtlicher Befugnisse verwendet werden dürfen, bleiben diese den Nachrichtendiensten vorbehalten (NOSINT). Dies zeigt, dass hier das primäre Unterscheidungskriterium zwischen Nachrichtendiensten und der Öffentlichkeit die rechtlichen Befugnisse und nicht die Fähigkeiten sind. Ausserdem zeigt es, dass dennoch in zwölf theoretischen Fällen die Leistungserbringung den Nachrichtendiensten vorbehalten (NOSINT) bleibt, sich aber immerhin drei theoretische Fälle der nichtstaatlichen Erbringung einer Nachrichtendienstleistung für den Staat (OSINT) ergeben. Es sind schliesslich diese drei Fälle, die aufgrund gegenüber den Nachrichtendiensten überlegener Fähigkeiten oder Ressourcen der spezialisierten Öffentlichkeit einer genaueren Betrachtung zur Optimierung der nachrichtendienstlichen Leistungserbringung bedürfen.

NOTIZEN

Die allgemeine Öffentlichkeit hat keine hinreichend speziellen Fähigkeiten oder Ressourcen im Vergleich zu den Nachrichtendiensten, um eine auftragsorientierte Nachrichtendienstleistung für den Staat zu erbringen. OSINT kann deshalb nur innerhalb der Nachrichtendienste oder einer hinreichend spezialisierten Öffentlichkeit erbracht werden. Aufgrund einer wenigstens teilweisen Überlegenheit der Öffentlichkeit hinsichtlich relevanter Fähigkeiten und Ressourcen, scheint es geboten, diese unter den notwendigen Vorsichtsmassnahmen zur Leistungserbringung für den Staat heranzuziehen.

Quellenkunde

Die Vielfalt und das Volumen offen zugänglicher Quellennetze und potentieller Informationskanäle machen eine akkurate methodische Erschliessung des verfügbaren Materials unverzichtbar. Erst durch eine verbindliche Systematisierung vor allem der Quellenkritik mithilfe des Handwerkszeugs der Geschichtswissenschaft und ihrer Hilfsdisziplinen können analytische Bewertungen als reproduzierbar, Quellen wiederum als authentisch und aussagekräftig gelten und damit einem objektivierbaren Informationsbedarf gerecht werden. Die Ausbildung und stete Aktualisierung eines historiographisch soliden, das heisst theoriegeleiteten Quellenbewusstseins muss daher nicht zuletzt im Sinne der Qualitätswahrung eines spezifischen Informationsproduktes (auch jenseits akademischer Forschung) jeder Beschaffung und Auswertung von Quellen vorausgehen.

Quellen, worunter Textquellen die wichtigste, jedoch bei weitem nicht einzige geschweige denn grösste Gruppe darstellen, sind Repräsentationen und Manifestationen vergangenen Geschehens, transportiert, sicht-, hör- und lesbar gemacht mithilfe bestimmter Medien als Tradition (intentionell weitergegeben) oder Überrest (nicht-intentionell überliefert). Sie bilden fragmentarisch und narrativ verengt Vergangenheit ab und sind in deskriptiver wie normativer Hinsicht zugleich Materialbasis und Kontrollinstanz für ihre Exegese. Insbesondere als offen verfügbares und somit öffentlich nachvollziehbares Überprüfungskriterium für ggf. sicherheitssensible, nicht aus offenen Quellen beschaffte Information ist eine sorgfältige wissenschaftliche Interpretations- und Reflexionspraxis alternativlos. Während daraus resultierende analytische Urteile immer vorläufig, also revidierbar sind und schwerlich je die Gesamtheit relevanter Quellen unvoreingenommen in Betracht ziehen können, müssen eigene Rechercheprämissen und inhaltliche Vorverständnisse und Befangenheiten ständig überprüft, angepasst, möglicherweise widerlegt und verworfen werden. Dass man vorrangig das sucht, was man bereits kennt oder erwartet, wirkt solcher Methodenkritik freilich entgegen und ist durch interdisziplinäre Anstrengungen und den engen Austausch von Beschaffung und Auswertung abzumildern. Der Suchexperte muss gleichermassen nachgewiesene Kenntnis von zielführenden Suchtechniken und -strategien wie vertiefte inhaltliche Kenntnisse vom Gegenstand seiner Arbeit haben. Eine rein technologiezentrierte Ausrichtung des OSINT-Arbeitsplatzes kann den Ansprüchen an belastbare, die politische Entscheidungsfindung und Meinungsbildung sekundierende, zeitkritische Informationsprodukte kaum genügen.

Nun werden Quellen per se erst nach ihrer Materialisierung oder *Dinglichkeit* verfügbar, je näher, zeitlich und räumlich, Geschehen und Beschreibung beieinander liegen, desto stärker sind sie in der Betrachtung, Rekonstruktion und Kontextualisierung zu gewichten. Als besondere Herausforderung erweist sich hier die Ermittlung des Ursprungs der Überlieferung, die Annäherung der *Information null* und die Identifikation ihres Urhebers, der massgeblich Rückschlüsse auf die Verlässlichkeit und Glaubwürdigkeit von Information noch vor etwaigen Übersetzungs- und Übertragungsverlusten zulässt. Da auch Primärquellen nicht notwendig identisch mit der Information, die sie beinhalten, sind (es sei denn, das Medium ist die Information), ist eine von vornherein eindeutige Verortung von philologischem und hermeneutischem Erkenntnisinteresse und der respektiven Arbeitstechniken zwingend.

Erst nach der standardisierten Registrierung der Quellenlage und dem Vergleich mit weiteren Quellen zur Einordnung von Originalität, Plausibilität und Verwertbarkeit der Information, also der Sicherung und dem Befund der Quelle, folgt deren Deutung und Interpretation.

Es wird zwischen äusserer, das heisst formaler, und innerer, das heisst inhaltlicher Quellenkritik unterschieden. Der Historiker Ernst Bernheim gibt folgenden Fragekatalog für die Anwendung äusserer Kritik vor:

NOTIZEN

„1. Entspricht die äussere Form der Quelle, die in Frage steht, der Form, welche den als echt bekannten sonstigen Quellen der Zeit und des Orts der angeblichen Entstehung jener Quelle eigen ist, in Bezug auf Formgebung, Sprache, Schrift, Stil, Komposition?

2. Entspricht der tatsächliche Inhalt der fraglichen Quelle dem, was uns sonst aus echten Quellen der Zeit und des Orts bekannt ist, wobei auch zu beachten ist, ob nicht etwa Tatsachen mit Stillschweigen übergangen oder unbekannt geblieben sind, welche ein wirklicher Zeitgenosse wissen musste und an solcher Stelle in solchem Zusammenhang nicht übergehen konnte, und ob sich nicht etwa in der Quelle Kenntnis von Tatsachen verrät, die zu einer späteren Zeit geschehen sind als zur Zeit der angeblichen Abfassung der Quelle?

3. Entsprechen Form und Inhalt der Quelle dem Zusammenhang und dem Charakter der Entwicklung, innerhalb deren dieselbe angeblich steht, bzw. passt dieselbe mit innerer Wahrscheinlichkeit dahinein?

4. Finden sich an der fraglichen Quelle Spuren künstlicher Mache, wie sie sich bei echten Quellen derart nicht finden?“

Im Hinblick auf die innere Quellenkritik, die das qualitative Verhältnis zwischen Zeugnis (Quelle) und Ereignis (Information) ergründet, sind wiederum Erwägungen zu vor allem sachlichen Elementen handlungsleitend.

Quellenarbeit im Bereich OSINT bedeutet die zeit–, ebenen– und bedarfsgerechte Herstellung neuer oder bisher nicht erfasster Sinnzusammenhänge durch die systematisierte Beschaffung und Auswertung offen zugänglicher Informationsstücke. Sie ist allein Mittel zum Zweck und muss am Erkenntniswert der Quelle für die jeweilige Fragestellung bemessen werden. Nur durch die kontinuierliche Kritik sowohl der Quelle selbst wie der Methode, die zu ihrer formalen Erschliessung und inhaltlichen Eingrenzung führt, hält das schlussendliche Informationsprodukt den Kriterien seriösen und professionellen Wissensmanagements stand. Die geschichtswissenschaftliche Methode bleibt damit auch im Umgang mit digitalen Quellen jedweder Art autoritativ.

NOTIZEN

Quellen und Verweise

Amazon Elastic Cloud
http://aws.amazon.com/de/ec2/#details

Studie Avanade Inc.
http://www.avanade.com/_uploaded/pdf/avanadethoughtleadershipcloudsurveyexecutivesummary833173.pdf

Cloud Automation Tools Test
http://www.networkworld.com/reviews/2010/060710-cloud-test.html

Ernst Bernheim: Lehrbuch der historischen Methode und der Geschichtsphilosophie
http://www.archive.org/details/lehrbuchderhistooobernuoft

Zotero Open Source Firefox Add-On
http://www.zotero.org/

Jumper Open Source Collaborative Search
http://www.jumpernetworks.com/

delicious Social Bookmarking
http://delicious.com/

U.S. Government Accountability Office (GAO):
Governmentwide Guidance Needed to Assist Agencies in Implementing Cloud Computing
http://www.gao.gov/new.items/d10855t.pdf

NOTIZEN

ISN
ETH Zurich

INTERNATIONAL RELATIONS AND SECURITY NETWORK

ETH Zurich | Leonhardshalde 21, LEH | 8092 Zurich | Switzerland
Tel: +41 (0)44 632 04 24 | Fax: +41 (0)44 632 14 13
www.isn.ethz.ch | osint@sipo.gess.ethz.ch

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich