Zum Auflösen zu blöd

Ein Kommentar von mir in der Jungle World: „Zum Auflösen zu blöd“ – Die Neonazis sind bei den Wahlen in Niedersachsen, Hessen und Hamburg sang- und klanglos untergegangen. Hier das ungekürzte Original-Manuskript:

Die Neonazis sind bei den Wahlen in Niedersachsen, Hessen und Hamburg sang- und klanglos untergegangen. In Hessen erreichte die NPD noch nicht einmal die Stimmenzahl, die nötig ist, um Wahlkampfkosten erstattet zu bekommen. In Hamburg war nur die Deutsche Volksunion (DJV) angetreten. Auch sie bekommt kein Geld aus der Staatskasse. In einigen Bezirken erreichte sie sogar noch weniger Stimmen als „Die Partei“, die deutsche Kampftruppen nach „Süd-Liechtenstein“ schicken will.

In den alten Bundesländern haben nur Rechtspopulisten – wie der längst Ronald Schill mit seiner Partei Rechtsstaatlicher Offensive – eine Chance, kurzfristig einen Zipfel der Macht zu erhaschen. Die DVU, die durch die Finanzkraft ihres alternden Vorsitzenden Gerhard Frey in der Lage gewesen wäre, die Bevölkerung mit brauner Propagandasoße zu überschütten, bleibt eine schrumpfende Politsekte. Neonazis in Parlamenten sind also ein ostdeutsches Phänomen.

Das Geld Freys eröffnete dem ultrabraunen Milieu den zumindest propagandistischen Zugang zu Nicht- oder Protestwähler, denen es egal ist, was sie ankreuzen, wenn es nur die „Etablierten“ ärgert. Damit ist es vorerst vorbei. Den unpolitischen Protest scheint jetzt „Die Linke“ aufgesogen zu haben. Die größte Leistung Oskar Lafontaines im Westen ist es, dieses Milieu zu neutralisieren. Schill und Schönhuber hätte keine Chance gegen den wortmächtigen Bonsai-Napoleon.

Die NPD allein ist im Westen nicht in der Lage, die Klientel zu erreichen, die ihr noch in den sechziger Jahren in Südwestdeutschland zweistellige Wahlergebnisse beschwert

hatte. Sie stützt sich vorwiegend auf die militanten Aktivisten der so genannten „freien Kameradschaften“ und auf Teile der rechten Jugendkultur. Im Beitrittgebiet ist das anders: Die NPD hat vor allem in Kleinstädten verankert. Die Nazi-Klientel dort ist aus ökonomischer Sicht kleinbürgerlich, aber viel weniger abgesichert als vergleichbare Milieus im Westen, daher leichter zu radikalisieren.

Das Wahlergebnis bedeutet nur etwas für das Machtgefälle zwischen den beiden konkurrierenden Nazi-Parteien und das Zweckbündnis „Deutschlandpakt“. Die NPD ist in einer Zwickmühle: Modernisiert sie sich wie die italienischen Neofaschisten, um für andere und neue Wählerschichten akzeptabel zu sein, müsste sie ihre Aktivisten abstoßen. Verließe sie sich auf ihre ostdeutschen Stammwähler, kann sie den Westen abschreiben. Der „Deutschlandpakt“ war ein Versuch, das zu ändern – und der ist wohl endgültig gescheitert, zumal Frey als Geldgeber in naher Zukunft schon aus biologischen Gründen ausscheiden wird.

Das Wahlverhalten der Deutschen ist seit Jahrzehnten unflexibel und relativ konstant, trotz zahlreicher soziologischer Unkenrufe, die Wählerinnen und Wähler entschieden sich immer unberechenbarer. Als Politsekte und als Hefe im nur konjunkturell zu bräunenden Teig der politischen Mitte hat die NPD keine Chance, weder in einem Stadtstaat wie Hamburg noch mit einem Wahlkämpfer wie Koch, der die Parolen der NPD volkstümlicher an die Wähler gebracht hat als das Original, noch in Niedersachsen, wo sich niemand mehr an politische Inhalte des Wahlkampfs erinnern kann.

Den Kadern der NPD und der DVU bliebe nur eine Chance, mehr politischen Einfluss zu bekommen als jetzt: Das zu tun, was ihnen die Maoisten von der KPD 1980 vormachten – die Partei aufzulösen und woanders unterzuschlüpfen. Aber dazu sind die Nazis zum Glück zu blöd.

Schlechte Karten für „Bundestrojaner“

Das Urteil des Bundesverfassungsgerichts, das Verfassungsschutzgesetz in Nordrhein-Westfalen für nichtig zu erklären, ist salomonisch und listig: Es gestattet allen Beteiligten, das Gesicht zu wahren. Erst im Kleingedruckten – in der ausführlichen Begründung – wird deutlich, dass die juristischen Hürden für die vom Bundesinnenministerium gewünschten „Online-Durchsuchungen“ fast unüberwindbar hoch sind.

Das neu eingeführte Gundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme als Teil des allgemeinen Persönlichkeitsrechts schließt einige juristische Lücken, die sich laut Gericht aus „neuartigen Gefährdungen“ im Zuge des „wissenschaftlich-technischen Fortschritts“ ergeben. Die durch das Grundgesetz garantierte „freie Entfaltung der Persönlichkeit“ musste exakter gefasst werden, weil Computer dafür eine immer größere Bedeutung erlangt haben, insbesondere

in vernetzten Systemen. Das ist an sich nichts Neues. Interessant ist jedoch, dass das Bundesverfassungsgericht es für fragwürdig hält, prophylaktisch Informationen über Personen zu sammeln:

„Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen“.

Daraus ergebe sich ein „erhebliches Schutzbedürfnis“, dem im Urteil Rechnung getragen wird. Der Einzelne sei darauf angewiesen, wenn er sich im Sinne des Grundgesetzes frei entfalten wolle, dass auch der Staat die Integrität und Vertraulichkeit informationstechnischer Systeme achte.

Der Schutz der „Persönlichkeit“ wird durch das Urteil erweitert auf die Technik, die die Person benutzt, um ihr Leben zu gestalten. Dazu passt, dass die Wohn-, Betriebs- und Geschäftsräume, die durch das Urteil zum Großen Lauschangriff vor dem Zugriff des Staates grundsätzlich geschützt wurden, jetzt auch die genutzten Rechnersysteme umfassen. Setzt sich jemand mit seinem Laptop in ein Cafe, gehört dieser automatisch zum „Kernbereich der privaten Lebensgestaltung“, in dem der Staat nicht einfach so herumschnüffeln darf. Der Bundesverfassungsgericht geht sogar ins Detail, Keylogger zu erwähnen und die elektromagnetische Abstrahlung des Computers, die man abfangen und auslesen könnte.

Selbst das bisherige Recht auf informationelle Selbstbestimmung ging dem Bundesverfassungsgericht nicht weit genug, weil heute jeder darauf angewiesen sei, Computer zu benutzen.

„Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus."

Das höchste deutsche Gericht beweist in seinem Urteil mehr technischen Sachverstand und hat investigativer zum Thema recherchiert als die meisten deutschen Medien. Es räumt auch gleich mit einigen urbanen Legenden auf. Hat es schon eine „Online-Durchsuchung" privater Rechner gegeben? Es sei nichts über die Technik der bisherigen „Online-Durchsuchungen" und über deren Erfolge bekannt. Die Präsidenten des BKA und des Verfassungsschutzes hatten keine Aussagegenehmigung. Das Bundesinnenministerium hatte auch in den Medien immer ausweichend reagiert und auf die Fragen des Bundesjustizministieriums geantwortet, die dazu nötigen Programmen würden erst noch entwickelt.

Im Verfassungsschutzgesetz Nordrhein-Westfalen findet sich die wolkige Formulierung, man wolle heimlich auf „informationstechnische System" zugreifen. Noch schwammiger ist der „Zugriff auf Internet-Festplatten„. Von einer „Online-Durchsuchung" war ursprünglich nicht die Rede. Letztlich lässt sich nicht mehr klären, ob der Gesetzgeber von Anfang an beabsichtigte, auch private Rechner durchsuchen zu lassen. Das Bundesverfassungsgericht hat die Diskussion kurz und bündig beendet. Nicht ganz humorlos wird erklärt, sowohl ein einzelner Rechner als auch das Internet als solches sei jeweils ein „informationstechnisches System".

„Unter einem heimlichen Zugriff auf ein informationstechnisches System ist demgegenüber eine technische Infiltration zu verstehen, die etwa Sicherheitslücken des Zielsystems ausnutzt oder über die Installation eines Spähprogramms erfolgt. Die Infiltration des Zielsystems ermöglicht es, dessen Nutzung zu überwachen oder die Speichermedien durchzusehen oder gar das Zielsystem fernzusteuern. Die nordrhein-westfälische Landesregierung spricht bei solchen Maßnahmen von einer clientorientierten Aufklärung des Internet. Allerdings enthält die angegriffene Vorschrift keinen Hinweis darauf, dass sie ausschließlich Maßnahmen im Rahmen einer am Server-Client-Modell orientierten Netzwerkstruktur ermöglichen soll.“

Da der heimliche Zugriff auch auf private Rechner definitiv nicht ausgeschlossen sei, müsse man auch über die „Online-Durchsuchung“, wie sie allgemein diskutiert werde, urteilen.

Spannend ist das Urteil vor allem in den Passagen am Schluss, die die Ausnahmen regeln. Der Schutz des „Kernbereichsschutz“ wird aufgeweicht. Bisher mussten Lauscher die Mikrofone auschalten, wenn die Verdächtigen anfingen zu beten oder über Sex redeten. Praktisch war eine Überwachung kaum noch möglich. Das Bundesverfassungsgericht hat festgestellt, dass das im Prinzip auch für Computer gilt. Die aus technischer Sicht sehr

kühnen Thesen des Bundesinnenminsteriums, man könne einfach durch das Design der Software die Privatsphäre ausreichend schützen, ein Spionage-Programm werde keine anderen Programme des betroffenen Rechers beeinträchtigen und diesen nicht verändern, glaubt das Bundesverfassungsgericht nicht. Es sei „praktisch unvermeidbar“ bei einem heimlichen Zugriff, wenn er bei einem technisch unbedarften Verdächtigen funktioniere, auch an Daten zugelangen, die die Ermittler weder zur Kenntnis nehmen noch verwerten dürfen. Einen „rein lesenden Zugriff infolge der Infiltration“ gebe es nicht.

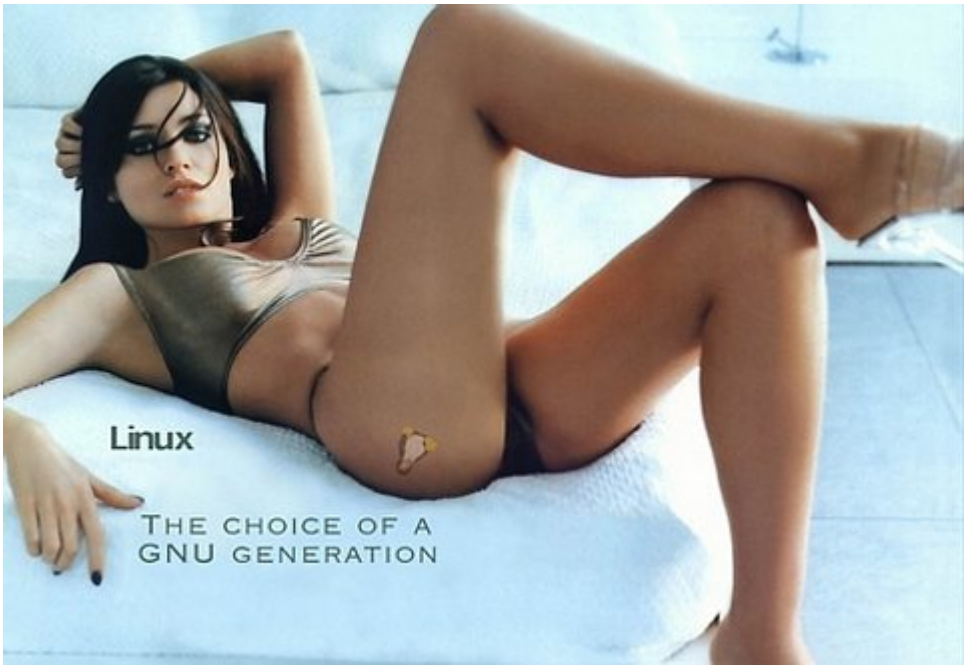
„Im Rahmen des heimlichen Zugriffs auf ein informationstechnisches System wird die Datenerhebung schon aus technischen Gründen zumindest überwiegend automatisiert erfolgen. Die Automatisierung erschwert es jedoch im Vergleich zu einer durch Personen durchgeführten Erhebung, schon bei der Erhebung Daten mit und ohne Bezug zum Kernbereich zu unterscheiden. Technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte.“

Das Bundesverfassungsgericht hat zur Kenntnis genommen, dass sich jeder vor einer „Online-Durchsuchung“ schützen kann – es verweist ausdrücklich auf die einschlägige Literatur. Dennoch könnte man allein deswegen diese Methode nicht ausschließen. Die Schranken für eine Überwachung eines privaten Rechners sind aber sehr hoch: Es muss eine konkrete Gefahr vorliegen, die ein „überragend wichtiges Rechtsgut“ bedroht. Klar ist auch, dass eine heimliche „Online-Durchsuchung“ immer einen schweren Grundrechtseingriff bedeutet, für ein ein Richtervorbehalt jetzt gesetzt ist. Das bedeutet: Nur bei unmittelbarer Gefahr für Leib und Leben einer Person oder bei konkreter Bedrohung für „den Bestand des Staates oder die Grundlagen der Existenz der Menschen“ dürfen die Ermittler

über eine „Online-Durchsuchung“ anfangen nachzudenken.

„Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann. Dagegen wird dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitergehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird.“

Und wenn dann ein Richter dem zustimmte, bedürfe es noch besonderer Vorkehrungen, um den geschützten Privatbericht nicht zu behelligen. „Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben.“



Durch das Urteil rückt das Sicherheitsinteresse der Staates ein wenig näher an die einzelnen Menschen heran. Der so

genannte „Kernbereich“ des Privaten ist kleiner geworden, dafür um so sicherer. Ein bloßes Gesetz schützte wenig vor privaten und staatlichen Datenkranken; ein Grundrecht jedoch, das als solches vom Bundesverfassungsgericht definiert ist, kann man kaum außer Acht lassen.

Die Hausaufgabe, die das Gericht dem Bundesinnenminister aufgegeben hat, ist so gut wie unlösbar, zumal eine Online-Überwachung durch die Polizei und das Bundeskriminalamt noch schwieriger ist als durch den Verfassungsschutz, der seine Daten für sich behalten kann. Die Ermittler hätten jedoch vor Gericht das zusätzliche Problem, beweisen zu müssen, dass die gefundenen Beweise auch echt sind. Möglicherweise, so steht es geheimnisvoll im Urteil, sei der „Beweiswert der Erkenntnisse gering“: Eine
„technische Echtheitsbestätigung der erhobenen Daten“ setze grundsätzlich „eine exklusive Kontrolle des Zielsystems im fraglichen Zeitpunkt voraus“. Und das muss man erst einmal technisch umsetzen und anschließend einem Richter beweisen – schlechte Karten für jede Art und Version eines „Bundestrojaners“.

Dieser Artikel von mir erschien am 27.02.2008 auf Telepolis.

Polit-Choreografie auf dem Balkan

Das Parlament des Kosovo hat am 17.02. in einer Sondersitzung die Unabhängigkeit der serbischen Provinz ausgerufen. Der – neben Albanien – zweite „albanische“ Staat auf dem Balkan kann allein wirtschaftlich nicht überleben. Aber darum geht es den heimlichen Geburtshelfern USA und EU nicht – sie verfolgen

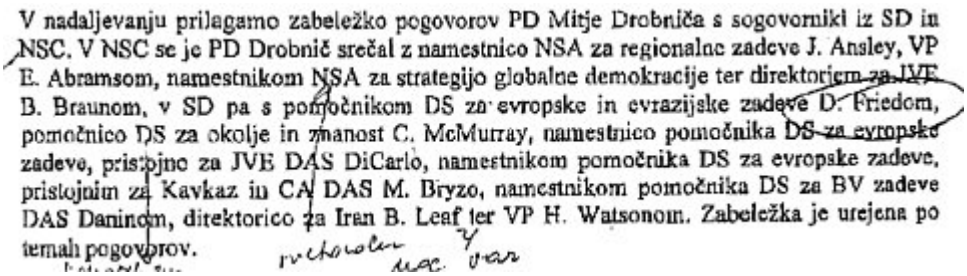
eigene Interessen.

Am 29.01. wartete die unabhängige und auflagenstärkste slowenische Zeitung *Delo* mit einem echten Scoop auf: Sie publizierte das Protokoll von Gesprächen zwischen Mitja Drobnič, dem politischen Direktor des slowenischen Außenministeriums, mit diversen US-Diplomaten – Vertretern der Regierung und des Nationalen Sicherheitsrates, unter anderem mit Daniel Fried, dem Staatssekretär im Außenministerium für europäische und eurasische Angelegenheiten. Die Gespräche zeigen, wie die USA den Fahrplan zur Unabhängigkeit des Kosovo während der EU-Ratspräsidentschaft Sloweniens durchzusetzen planten und bis in Detail vorgaben. Die US-Diplomaten schlagen vor, das Parlament des Kosovo möge die Unabhängigkeit an einem Sonntag erklären – wie es jetzt geschah. Russland habe dann keine Zeit mehr, den UN-Sicherheitsrat einzuberufen. Wenn die ersten Staaten den Kosovo anerkannt hätten, gebe es ohnehin kein Zurück mehr.

„Die Vereinigten Staaten vermieden einstweilen Aussagen zur Unabhängigkeit des Kosovo, werden aber nach der Proklamierung der Selbständigkeit durch die Regierung des Kosovo dann unter den ersten Regierungen sein, die die Selbständigkeit anerkennen werden. Die USA strebten an, daß der Kosovo in den ersten Tagen von möglichst vielen Ländern außerhalb der EU anerkannt werde. Die Vereinigten Staaten würden eine starke Lobby-Arbeit in Japan, der Türkei sowie den Arabischen Ländern betreiben, in Ländern also, die ihre Bereitschaft gezeigt hätten, den Kosovo ohne Zögern auch anzuerkennen."

Peinlich ist der Inhalt der Gespräche für die slowenische Regierung, weil sie mehr oder weniger zu einem Befehlsempfänger degradiert wird. Daniel Fried legte Slowenien nahe, als erster Staat den Kosovo anzuerkennen. Die Rolle des neutralen Vermittlers zwischen Serbien und seinen abtrünnigen Provinzen kann die Regierung in Ljubljana jetzt nicht mehr besonders glaubwürdig vertreten. Die US-Diplomaten lassen auch keinen Zweifel daran, dass in den Deklarationen der Europäischen Union die Interessen der USA mit formuliert werden sollen. Georg Bush wünscht sich zum Beispiel, dass „Kuba und Venezuela" als „problematische Staaten" und der „Terrorismus" jeweils erwähnt werden.

Diese Vorgeschichte wurde von den deutschen Medien bei der Berichterstattung über die Unabhängigkeitserklärung fast ausnahmslos verschwiegen. Am 15.02. publizierte Ekkehard Sieker, langjähriger Fernsehjournalist bei Monitor und heute verantwortlicher Redakteur der Website hintergrund.de, eine deutsche Übersetzung). Man muss Siekers Theorien zu anderen Themen nicht beipflichten, aber die deutsche Version des Textes entspricht dem, was auch die österreichische Zeitung *Standard* in Auszügen veröffentlichte und worüber *Die Presse* schon am 29.01. berichtete.



V nadaljevanju prilagamo zabeležko pogovorov PD Mitje Drobniča s sogovorniki iz SD in NSC. V NSC se je PD Drobnič srečal z namestnico NSA za regionalne zadeve J. Ansley, VP E. Abramsom, namestnikom NSA za strategijo globalne demokracije ter direktorjem za JVE B. Braunom, v SD pa s pomočnikom DS za evropske in evrazijske zadeve D. Friedom, pomočnico DS za okolje in znanost C. McMurray, namestnico pomočnika DS za evropske zadeve, pristojno za JVE DAS DiCarlo, namestnikom pomočnika DS za evropske zadeve, pristojnim za Kavkaz in CA DAS M. Bryzo, namestnikom pomočnika DS za BV zadeve DAS Daninom, direktorico za Iran B. Leaf ter VP H. Watsonom. Zabeležka je urejena po temah pogovorov.

Die Protokolle haben in Slowenien eine mittlere Staatskrise ausgelöst. Mitja Drobnič musste zurücktreten. Ein parlamentarischer Untersuchungsausschuss widmet sich der Frage, wo die undichte Stelle war, die die Medien informierte. Der Computer des hochrangigen Diplomaten Marjan Setinc wurde beschlagnahmt, weil Setinc in Kontakt zu einer Journalistin der *Dnevnik* stand – die Zeitung hatte die Protokolle ebenfalls publiziert. In Slowenien rätselt man zur Zeit darüber, wer im Laufe der „Hexenjagd“ im Außenamt bei wem die Telefone abgehört haben könnte.

Aus den Protokollen lassen sich die Prinzipien der Lobby-Arbeit der USA auf dem Balkan erkennen. Die Regierung Bush macht Druck auf Slowenien, möglichst bald innerhalb der Europäischen Union vollendete Fakten zu schaffen. Einige Mitgliedstaaten gelten als zögernd, insbesondere die Niederlande geben den Hardliner gegen die Autonomie-Pläne ohne Zustimmung der UN (laut Resolution 1244 des UN-Sicherheitsrates. Staatssekretär Fried soll sich bemühen, den UN-Generalsekretär Ban Ki-moon dazu zu bewegen, sich positiv zu einer Mission der EU in den Kosovo zu äußern. Es soll vermieden werden, dass der UN-Sicherheitsrat sich zuungunsten einer Unabhängigkeit des Kosovo einmischt.

„Slowenien muss aber innerhalb der EU eine baldige Entsendung der Mission erreichen. (…) DiCarlo: Es gilt die Überzeugung, dass Ban schwerlich zur Übernahme der Mission aufrufen kann, bevor es zur Unabhängigkeitserklärung (…) kommt. (…) Nach der Unabhängigkeitserklärung muss es sofort zur Anerkennung kommen, weil der Generalsekretär nur dann feststellen kann, dass sich die Situation an Ort und Stelle verändert hat, und

er die EU aufrufen kann, die (Kosovo-)Mission zu übernehmen. (…) Ban müsste (dann) nur betonen, „facts on the ground have changed“ und die EU einladen, ihre Mission zu entsenden. Ban braucht dafür keine Entscheidung des UNO-Sicherheitsrates.“

Die Methode ähnelt der Situation unmittelbar nach der Auflösung des ehemaligen Jugoslawiens beim Beginn des Kroatienkriegs 1991. Damals erkannte Deutschland Kroatien als einer der ersten Staaten an. Fast gleichzeitig unterzeichnete Kroatien ein Stabilisierungs- und Assoziierungsabkommen mit der Europäischen Union, das den freien Zugang zum Europäischen Binnenmarkt sicherte. Das Prinzip ist: Entweder eine Regierung unterwirft sich letztlich den Regeln der europäischen Union, wie in der Thessaloniki Agenda vom Juni 2003 präzisiert, oder sie wird wirtschaftlich in jeder Beziehung an den Rand gedrückt. Die mehr symbolische Affinität Serbiens zu Russland – aus historischen Gründen – kann letztlich nicht gegensteuern.

Politische Moral spielt keine Rolle. Es ist ein offenes Geheimnis, dass es im Kosovo, dem ehemals ärmsten Teilstaat Jugoslawiens nur zwei florierende Wirtschaftszweige gibt: Den Menschen- und den Drogenhandel. Noch vor zehn Jahren definierte die US-Regierung die so genannten „Unabhängigkeitskämpfer“ der Kosovo Liberation Army (KLA bzw.

UÇK als – wenn auch unbedeutende – Terrororganisation. Plötzlich wandelte sich die UÇK in den Augen des CIA zur Befreiungsarmee, obwohl deren Haupteinnahmequelle der Heroin-Schmuggel nach Westeuropa war. Die *London Times* formulierte im Juli 1999: „Kosovo is Mafia's ‚heroin gateway to West'". Die *Berliner Zeitung* zitierte am 04.03.1999 Quellen, die die bisherigen Einkünfte der UÇK auf über 900 Millionen Mark schätzte. Die Hälfte der Summe stammte aus dem Drogenhandel, die andere Hälfte von einer Art „Kriegssteuer", die die UÇK von den ausgewanderten Kosovo-Albanern eintrieb.

Das Strategic Issues Research Institute (SIRIUS) hat die Presseberichte internationaler Medien zu diesem Thema zusammengestellt – „on KLA-Kosovo-Drugs-Mafia and Fundraising". Die *Washington Post* berichtete am 26.05.1998 über die Unterstützung der mafiösen Banden und der UÇK im Kosovo durch albanische Einwanderer- rund eine halbe Million Albaner lebt in den USA. Die *Romania Libera* schrieb am 30.07.1998: „The Albanian terrorism and separatism obscures the geopolitical and the strategic dimension known only by some. In the offices of the Great, the Balkans is considered to have the deciding role of the stability or instability of Europe. Within this context, Kosovo and Macedonia seem to be in possession of keys of stability in the Balkans. Phantom Government" of the so-called Kosovo Republic -still unrecognised by any state – has its seat in Ulm near Bonn, in Germany. The leader of this phantom „republic" – Buyar Bukoshi – receives significant „donations", later to be deposited in the Swiss banks or secret safes. Bukoshi himself, with his family, lives in Ulm. Meaning, far away from the bloodshed in Kosovo. Contrary to the leader, Ibrahim Rugova, who has not left the region and is looking forward to the US State Department support. In 1997, the Carnegie Foundation" invited Rugova to USA and introduced him to the public through mass media in the right way. If Bukoshi is „the Germany man", Rugova is „the American man".

.

Der Artikel ist in seinen wesentlichen Aussagen immer noch aktuell. Die Interessen der USA auf dem Balkan sind jedoch nur punktuell identisch den denen der Europäischen Union. Die Bush-Regierung plant schon seit Jahren, sich den strategischen Korridor Bulgarien-Mazedonien-Albanien zu sichern – den Weg des Öls vom Schwarzen Meer zur Adria. Die Kleinstaaterei und wirtschaftliche Abhängigkeit ist da von Vorteil. Pläne eines Großalbanien, wie sie Teile der aufgelösten UÇK vertraten, schaden den ökonomischen Interessen, die sich die Rohstoffe sichern wollen. Eine geplante Pipeline etwa führt vom bulgarischen Hafen Burgas bis Vlora in Albanien und wird von der Albanian Macedonian Bulgarian Oil Corporation verwaltet, die in den USA registriert ist. AMBO steht in enger Verbindung mit dem internationalen Konzern Halliburton. US-Vizepräsident Dick Cheney war zeitweilig Aufsichtsratpräsident.

AMBO steht in direkter Konkurrenz zu dem französischen Öl-Multi Total. So erklärt sich auch die Passage in dem geheimen Protokoll: „Drobnič bezeichnete im Weiteren die Aussage des französischen Präsidenten Sarkozy als problematisch, der den serbischen Weg in die EU mit der Lösung des Kosovo-Konflikts verbunden habe.“

Kurz vor der Bombardierung Jugoslawiens im Jahr 1999 sagte Bill Clintons Energieminister Bill Richardson laut *The Guardian* vom Februar 2001, es gehe darum, Amerikas Energieversorgung zu sichern. „Wir haben in der kaspischen Region erheblich politisch investiert, und es ist sehr wichtig

für uns, daß die Karte der Pipelines und die Politik gleichermaßen stimmen."

Die USA sind auf ihrem Weg, die Karte des Balkan dem Weg des Öls anzugleichen, mit der Unabhängigkeit des Kosovo wieder ein Stück näher gekommen.

Dieser Artikel von mir erschien am 18.02.2008 auf Telepolis. Vgl. auch „Konfliktherd Balkan" (23.02.2008) von Florian Rötzer und „Auf dem Weg in die Spaltung" (28.02.2008) von Boris Kanzleiter.

Geheimdienst-Nummer

Der Westen: „Die klassische Geheimdienst- Nummer ist denkbar"

> *Burkhard Schröder etwa, der in seinem ‚Online-Tagebuch, über Politik, Wissenschaft und Medien seinen Angaben nach investigativ berichtet, schreibt in einem Telepolis-Artikel: ‚Bei der Online-Untersuchung handelt es sich also um eine reine Wunschvorstellung und mitnichten um eine real existierende Methode.' So genannte Bundestrojaner seien noch nie angewendet worden.*

Das heisst *nicht*, sie sei nicht möglich, sondern nur, dass sie noch nicht praktiziert worden ist.

> *‚Zu sagen, Online-Durchsuchungen sind nicht möglich, ist Blödsinn‘, klärt Dr. Christoph Wegener, Spezialist im Bereich IT-Sicherheit an der Ruhr-Universität Bochum, auf. ‚Durchsuchungen sind tendenziell möglich‘, nennt jedoch im gleichen Satz schon das Problem: ‚Man kann sich davor schützen.‘ Das kann der Verdächtige also auch tun.*

Was denn nun? Sind sie möglich, wenn man sich schützen kann? Oder deswegen nicht?

Schlechte Karten für „Bundestrojaner“

Ein Artikel von mir auf Telepolis: ‚Schlechte Karten für „Bundestrojaner'“.
Nachtrag 28.02: Der Link zum Urteil ist falsch, darauf hat ein aufmerksamer Leser hingewiesen.

Hausaufgaben für Wolfgang Schäuble

Ein Artikel von mir in der Netzeitung (27.02.2008): „Hausaufgaben für Wolfgang Schäuble“.

Polit-Choreografie auf dem Balkan

Ein Artikel von mir auf Telepolis (18.02.2008):“Polit-Choreografie auf dem Balkan“.

Anti-Terror-Kampf im Internet


Anti-Terror-Kampf im Internet

„Der Verfassungsschutz muss die Möglichkeit erhalten, auf Internet-Festplatten zuzugreifen, um inländische Terrorzellen aufzuspüren und zu beobachten", sagte Innenminister Ingo Wolf (FDP) zur WAZ.

Ich habe mir jetzt den Original-Artikel aus der WAZ besorgt, der den Medien-Hoax um die „Online-Durchsuchung“ maßgeblich beeinflusst hat. In meinem Telepolis-Artikel vom 06.02.2007 hieß es:

> *Wolf hat überhaupt nichts von „Online-Durchsuchungen“ gesagt. Im August 2006 heißt es im Heise-Newsticker korrekt nur, es solle jetzt das Internet überwacht werden. Die dort erwähnte Formulierung „Zugriff auf Internet-Festplatten“ stammt aus der Welt. Die wiederum bezieht sich auf ein Interview der WAZ vom 28.08.2006 mit Ingo Wolf: ‚Der Verfassungsschutz muss die*

> *Möglichkeit erhalten, auf Internet-Festplatten zuzugreifen, um inländische Terrorzellen aufzuspüren und zu beobachten.‘ Das ist allgemein formuliert und bedeutet gar nichts Konkretes. Was mit „Internet-Festplatten“ gemeint ist, kann man nur vermuten: Festplatten in den Rechnern der Provider, im Gegensatz zu privaten Festplatten, die manchmal offline sind?*

Aus den „Internet-Festplatten“ haben dann die Medien private Computer gemacht – und die urbane Legende des Behörden-Hackers war geboren. Demnächst mehr in einem größeren Werk…

Kapitalismus 2.0

Dieser Artikel erschien leicht verändert am 08.02.2008 unter dem Titel „Virtuelles Geld, reale Banken – und umgekehrt“ in der Netzeitung.

Es ist nicht immer eine Bank, wenn Bank draufsteht. Das mussten viele Nutzer der digitalen Welt Second Life schmerzlich erfahren: Gingko Financial, die bekannteste „Bank“, löste sich im September spurlos auf. 200 Millionen der Second-Life-„Währung“ Lindendollar waren weg – umgerechnet eine halbe Million Euro Einlagen. Der Gingko-„Banker“ Andre Sanchez alias Nicholas Portocarrero alias Michael Pratte konnte nicht belangt werden. Ein virtueller Schwarzer Freitag also? Nein: Reale Banken funktionieren in virtuellen Welten genausowenig wie die realen Marktgesetze. Das hindert Linden Lab, die Betreiberfirma von Second Life, dennoch nicht daran, mit seinen „Economic Statistics“ das Gegenteil zu suggerieren.

In Second Life kann man reales Geld ausgeben, etwa für den Kauf eines virtuellen Grundstücks, die dafür fällige monatliche „Steuer“ an Linden Lab, für die Textilien des Avatars, für Genitalien oder für Dienstleisungen wie Cybersex. Reale Dollar müssen dafür in Lindendollar umgetauscht werden. Das geht – mit wenigen Ausnahmen – nur über eine Kreditkarte oder ein Konto bei Paypal. Jeder Avatar trägt seine virtuelle Geldbörse immer bei sich, ohne dass sie in Gefahr wäre gestohlen zu werden oder an Wert verlöre.

Der Lindendollar ist jedoch trotz seines „Wechselkurses“ keine Währung, sondern nur ein Micropayment-System mit einem willkürlich von Linden Lab festgesetzten Wert, vergleichbar mit Microsoft Points, einer Verrechnungseinheit, mit der man zum Beispiel für den MP3-Player Zune Songs kaufen kann. Niemand braucht daher Banken in Second Life. Auch die „Börse“ in Second Life verschwand schon nach kurzer Zeit wieder im Nirwana.

Avatare können keine Verträge miteinander abschließen, die einklagbar wären, ohne den realen Menschen hinter der virtuellen Maske identifiziert zu haben. Die Nutzer in Second Life dürfen fast alles tun, solange keine ernsthaften

Beschwerden laut werden. Sie können andere betrügen, sich Vertrauen erschleichen und Lindendollar zu Wucherzinsen verleihen wie im Mittelalter.

Second Life ist aber keine Simulation der Welt, sondern imitiert nur bestimmte Aspekte der Realität. Niemand kann bei Streitfällen ein Gericht anrufen. Es gibt keinen Krieg: Politik kann nicht mit anderen Mittel fortgesetzt werden. Die Ökonomie stagniert nur auf dem Niveau eines Pfandleihhauses. Noch nicht einmal die Wirtschaft Venedigs in der Renaissance könnte realistisch nachgespielt werden, obwohl der reale Umsatz in und mit Second Life das Bruttosozialprodukt von Guinea-Bissau übersteigt. In der vituellen Welt gibt es weder Gewalt noch Diebstahl. Die wenigen Hacker-Angriffe auf das Hab und Gut der Avatare nutzten Lücken in der Zugangssoftware aus, die Linden Lab bekannt waren, aber nicht rechtzeitig oder aus Prinzip nicht geschlossen wurden – wie die Möglichkeit, Avataren, die fahrlässig Land weit unter dem üblichen Preis anbieten, ihr Territorium durch eine speziell programmierte Software („Bots“) wegzunehmen.

Es gab daher auch keine virtuelle Bankenkrise. Das Vermögen der so genannten virtuellen Geldinstitute war immer „Fiat money“ – ein Begriff aus der Volkswirtschaftslehre für Geld,

das nicht oder nur teilweise durch reale Werte gedeckt ist. Die „Banken“ konnten sich nur etablieren, weil die Betreiber Zinsen bis zu 40 Prozent versprachen, also Gutgläubige fanden, die an eine Art wundersame und magische Vermehrung des Lindendollar glaubten. Auch in der realen Welt findet so etwas immer wieder statt, bis hin zu Pyramidenspielen und schlichter Abzockerei.

Die Allgemeinen Geschäftsbedingungen von Linden Lab wären nach deutschem Recht ohnehin nichtig: Die kalifornische Firma behält sich vor, ihre Kunden jederzeit ohne Angabe von Gründen enteignen zu können – ohne sie dafür zu entschädigen. Linden Lab finanzierte seine 3D-Welt vor allem durch Risikokapital des Investors Benchmark Capital, will aber selbst kein Risiko eingehen und hat sich juristisch ungefähr den Status eines mittelalterlichen Raubritters gesichert. Keine deutsche Bank betreibt ihr ureigenstes Geschäft unter solchen Bedingungen.

Ab dem 22.1.2008 dürfen nur noch virtuelle Banken in Second Life ihre Dienste anbieten, die auch eine Lizenz im realen Leben vorweisen können. Dubiose „Firmen“ wie die Royal Bank of Whitfield – im Besitz eines deutschen Nutzers – oder die „Thomas Bank Deutsche Branche“ sind verschwunden. Nur die „Q110 Deutsche Bank“ ist virtuell präsent – mit einer Filiale, die der realen in der Friedrichstraße in Berlin-Mitte

nachgebaut ist. Das auf sechs Monate befristete Projekt soll als Test dienen, sich mit virtuellen Welten zu befassen, wie die Besucher die „Q110 Deutsche Bank“ wahrnehmen und was sie davon erwarten. „Das Ziel war es nicht, reale Konten anzubieten“, sagt der Avatar Hedge Koenkamp alias Oliver Ehrhardt im realen Leben. Die Filiale ist ein Pilotprojekt für die gefühlte „Bank der Zukunft“. Der Geldautomat der virtuellen Deutschen Bank macht etwas, wovon man in der Realität nur träumen kann: Er spuckt nach dem Zufallsprinzip fünf Lindendollar (0,01 Cent) an Avatare aus – ein Bonsai-Glücksspielautomat in pseudo-seriösem Outfit, den man in der realen Filiale der Deutschen Bank vergeblich sucht.

Auf den „Gelben Seiten“ von Second Life finden sich dennoch zahlreiche Banken, als verlangten die Nutzer, dass ihnen das, was virtuell nicht funktioniert, immerhin vorgegaukelt wird. Das New Yorker Unternehmen Coldwell Banker zum Beispiel besitzt eine – mittlerweile stark eingedampfte – virtuelle Niederlassung. Das Unternehmen ist aber keine Bank, sondern handelt vornehmlich mit Immobilien, die man auch virtuell begutachten konnte. Man kann dort Lindendollar auf ein Konto einzahlen, eine Art Pfand für den Kauf einer virtuellen Immobilie, das man ohne Zinsen nach einer Frist zurückbekommt. Auch das ist kein normales Bankgeschäft.

Einige Geldinstitute in Second Life sind seriös, aber trotzdem keine Bank. Sie nutzen die Tatsache aus, dass es schwierig ist, ohne Kreditkarte an das virtuelle „Spielgeld“ heranzukommen. Wer Lindendollar etwa bei ebay ersteigert, geht das Risiko ein, sein Vermögen sofort wieder zu verlieren, wenn sich herausstellte, dass es der Verkäufer mit einer gestohlenen Kreditkarte oder auf eine andere Art missbräuchlich erworben hat. Das deutsche Unternehmen Wirecard bietet eine Art virtuelle Prepaid-Mastercard an, die man bis zu einer gewissen Summe auch bar bei einer Bank auffüllen kann. Ohne PostIdent-Verfahren hat der User kein normales Girokonto, sondern ein eGeld-Account. Auch der Telelinden Cash Service aus Germering bei München offeriert, ohne Konto und Kreditkarte Lindendollar erwerben zu können.

Der „Bankencrash“ von Second Life beweist vor allem eines: Vertrauen in ein Geldinstitut ist gut, aber nur für das Institut, nicht für den Kunden. Kontrolle der Bank wäre besser, aber nicht von einem Raubritter, sondern von einer Bankaufsicht. Man darf gespannt sein, wie Linden Lab reagierte, wenn eine Bank mit staatlicher Lizenz aus Nigeria oder aus Angola eine virtuelle Niederlassung eröffnete.

„Andre Sanchez“, den ich noch im Artikel in der Netzeitung erwähnte, existiert vermutlich nicht, vgl. die ausführliche

Diskussion über die wahren Hintermänner der „Ginko Financial“ auf virtuallyblind.com (Benjamin Duranske, 13.08.2007):

„The reason I haven’t run this info on VB up to now is that I had – so far – been fairly convinced that the registrant, Michael Pratte, though affiliated with Ginko and someone who took money from it, was not the person who controls the ‘Nicholas Portocarrero’ avatar. I’ve known I could be wrong on this point, but I was never sufficiently convinced otherwise to run the data identifying Pratte. That all said, I’m intrigued by the above poster’s (confirmed) point that ginkosoft.com was registered in 2000 (well before Second Life was created).

That has to mean either:
1) Andre Sanchez (who controls the avatar ‘Nicholas Portocarrero’) met a guy in Second Life in early 2005 who already had a domain. Under this theory, I’m guessing the guy is ‘Hinoserm Rebus,’ Ginko’s technical guy, and an avatar probably controlled by Michael Pratte. That guy – Pratte/’Rebus’ (or some other avatar we don’t know about) owned a website called “ginkosoft.com” already, and he and Sanchez decided to name the bank “Ginko” because the site wasn’t being used for anything. They then bought ginkofinancial.com (in 2005), and Pratte/’Rebus’ (or whoever) registered that one too.
or…
2) There is no “Andre Sanchez” and the guy who owns both domains – Michael Pratte – ran Ginko and controls both the ‘Portocarrero’ and ‘Rebus’ avatars. If the second of the above options is true, and this whole story (Nicholas being inspired by a famous banker, etc.) is completely phony from the beginning, then it’d be pretty hard argue this wasn’t actually set up as a scam from day one. Also, for what it’s worth, it would be a lot easier to sue a guy who is in the U.S. (if Pratte… is Hinoserm… is Nicholas – he is now in Texas according to the Official Ginko Blog) than a guy in Brazil.“

Die Erlkönigin

Dieser Artikel erschien am 09.06.2002 auf Telepolis. Da die meisten Links nicht mehr funktionierten, soll er hier aktualisiert noch einmal publiziert werden.

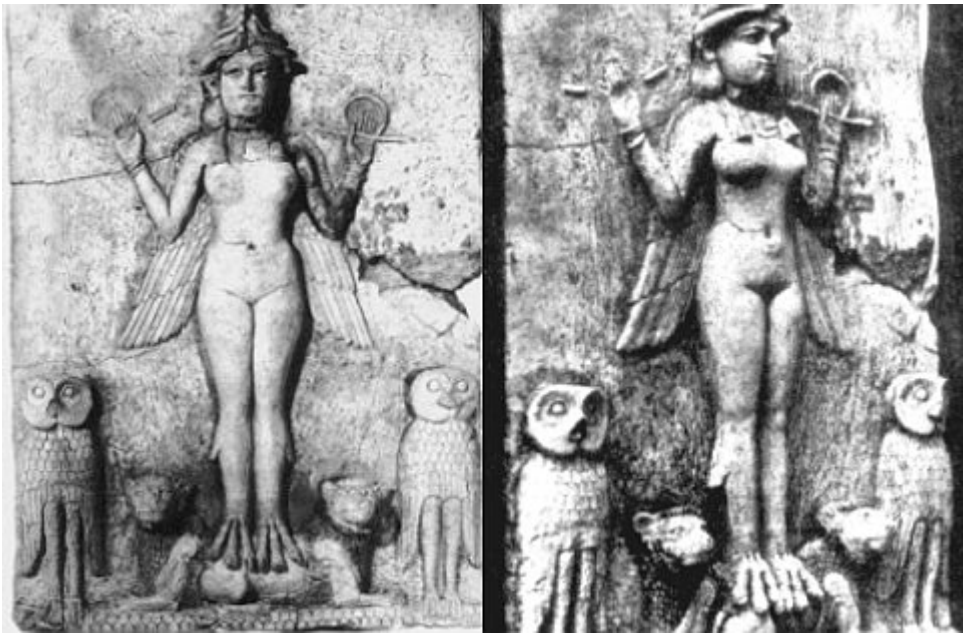
Der Erlkönig reitet wieder durch Nacht und Wind und durch die deutschen Medien. „André Ehrl-König“ ist das leicht zu enträtselnde Pseudonym für Marcel Reich-Ranicki in Martin Walsers neuem und mit Antisemitismen gespickten Roman „Tod eines Kritikers„. Und in den dürren Blättern des Feuilletons säuselt es von Herder, Goethe und „nordischer“ Mythologie, aus der die Figur des Erlkönigs angeblich stamme. Alles falsch.

Der Erlkönig treibt auch in der jüdischen Alltagsmythologie sein Unwesen, ist dort aber eine widerborstige Frau. Und die Figur beweist, dass sowohl Christentum als auch Judentum gemeinsamen Wurzeln im weiblichen Götterpantheon Alt-Mesopotamiens haben. Nur die keltischen Druiden wussten noch, wer der Erlkönig wirklich war, kommunizierten aber nur in einen Geheimsprache darüber, deren Entschlüsselung heutigen Kryptologen den Schweiß auf die Stirn treiben würde.

In Goethes Ballade aus dem Jahr 1782 fragte der verängstigte Knabe: „Siehst, Vater, du den Erlkönig nicht? Den Erlenkönig mit Kron‘ und Schweif?“ Die Macht des Dämons scheint auch Walser fasziniert zu haben. Stephan Ripplinger wirft Walser wohl zu Recht vor, mit der Analogie „Ehrl-König“ und Reich-Ranicki dem Juden an sich zauberische und tödliche Machenschaften zu unterstellen – ein klassischer antisemitischer Topos seit dem Mittelalter. Doch warum besitzt der Erlkönig „Krone und Schweif“ und warum raubt und tötet er kleine Jungen?

Goethes „Erlkönig“ liegt eine von Herder übersetzte dänische Ballade zugrunde – Erlkönigs Tochter. Das dänische Wort heißt „Ellerkonge“ (oder „elverkonge“) und bedeutet „Elfenkönig“. Generationen von Germanisten meinen, Goethe habe sich geirrt und falsch übersetzt. Selbst die Enzyclopedia Britannica und The Oxford English Reference Dictionary behaupteten das. Falsch: Goethe wusste genau, was er schrieb und warum er den Elfenkönig oder „Elbenkönig“ zu einem König der Erlen machte.

Die Worte „Ellerkonge“ oder Elberich („rich“ bedeutet „König“) und Alberich haben dieselbe ethymologische Wurzel. Der Zwerg Alberich ist der König der Unterwelt und taucht schon im deutschen Nationalepos Das Nibelungenlied auf. Die Wurzel „alb“ bedeutet ursprünglich „weiß“ und bezeichnet die Farbe als auch „die Frucht“. Das griechische Wort „alphos“ ist der „weiße Aussatz“ (lateinisch „albula“ – von „albus, „weiß“). Ein ganzes Kapitel des Romans „Moby Dick“ von Herbert Melville über die Jagd auf den weißen Wal widmet sich der Frage, warum die Farbe Weiß unheimliche Assoziationen weckt…



Alphito

Das ist kein Zufall. Dieses sprachgeschichtliche Indiz verweist auf eine der ältesten Mythen des Mittelmeerraums: die Legende von der unheimlichen Göttin Alphito, der die Gerste geweiht war – „alphiton“ bedeutet Gerste. Alphito strafte in vorgriechischer Zeit die, die sie nicht mochte, mit der Hautkrankheit Lepra. Die Worte „Albtraum“ und „Albino“ (für „weiß“) wurden aus dem Namen dieser Göttin abgeleitet – auch der Flussname „Elbe.“

Sogar die Bibel berichtet verschlüsselt von Alphito: Im 3. Buch Mose, Vers 10 wird angeordnet, dass derjenige, der vom Aussatz (Lepra) geheilt wurde, einen Scheffel Gerste (im Originaltext: Gerstenmehl, bei Luther wird Semmelmehl daraus) opfern musste – ursprünglich ein Dank an die Göttin, die an der Krankheit Schuld war. Das Albdrücken ist ein Synonym für Nachtmahr, früher auch für Inkubus, also einen Dämonen.

Der römische Schriftsteller Plinius kannte noch das alte Wort „Albion“ für die „Britischen Inseln“, und der Historiker Nennius, der um 820 vor Christus die Historia Brittonnum veröffentlichte, behauptete, die Bezeichnung „Albion“ stammte von „Albina“, der Weißen Göttin der griechischen Danaiden, den legendären Vorfahren der Mykener.

Was haben aber die Elfen und die Erle gemeinsam? Der dänische „Ellerkonge“ sei in Wahrheit der altenglische Gott Bran, der „König der Erlen“, schreibt Robert von Ranke-Graves in „Die Weiße Göttin„. Des Rätsels Lösung verbirgt sich in einer uralten walisischen Sage, der Schlacht der Bäume, die von keltischen Druiden und später von Minnesängern mündlich überliefert wurde. Diese Sage schildert in verschlüsselter Form die Eroberung einen Totenstadt auf der Ebene von Salisbury während der Invasion Britanniens durch die Kelten – den Vorfahren der Gallier – in der Eisenzeit. Die Götter der Sieger und Besiegten kämpfen als Bäume gegeneinander. Nur die Eingeweihten konnten Jahrhunderte später den Sinn der Story noch entschlüsseln.

Die keltischen Druiden benutzten dazu ein Fingeralphabet: der Buchstabe F (für „fearn“, die Erle) wurde mit der Spitze des Mittelfingers angezeigt, ähnlich wie in der heutigen Taubstummensprache. Julius Cäsar, der Eroberer Britanniens, beklagte sich später darüber, dass die Druiden nichts schriftlich niederlegten, sondern mittels geheimer Zeichen miteinander redeten und dass sie, was weder er noch spätere christliche Missionare verstanden, angeblich griechische Buchstaben verwendeten. Der englische Historiker Edmund Spenser behauptete 1596, die englischen Druiden hätten ihre Buchstaben von einem Volk, das vom Mittelmeer über Spanien nach Britannien gekommen sei.

Lilith

Ein weiteres Indiz dafür, dass die Druiden Mythen und Götter überlieferten, die von Einwanderern aus dem Mittelmeerraum stammten, findet sich in der Romance of Taliesin. Dort tritt Gwion auf, der bekannteste Barde des keltischen Mythos. Seine Gegenspielerin ist die finstere Göttin Cerridwen, die in dreifacher Gestalt erscheint und der der keltische Kupferkessel geweiht ist. Hinter Cerridwen verbirgt sich die altgriechische Göttin Alphito: Sie überwacht die Ernte der Gerste und verwandelt sich im Kult in eine weiße, leichenfressende Sau. Das altirische und walisische Wort „cerdd“ bedeutet „weiß“ oder „Zunahme“. Und in der spanischen Sprache und Folklore lebt Alphito alias Cerridwen heute noch weiter: „cerdo“ heißt Schwein, und der „Cerdaña“ ist der berühmte Gerste- und Getreidetanz der spanischen Pyrenäen.

Nur im französischen Arles hat sich ein Mysterienspiel der dreifachen Todesgöttin erhalten. Es wird Ende Mai unter dem Titel Die drei Marien der Provence gefeiert. Dieses Ritual wurzelt in einer christianisierten Deutung vorchristlicher Grabsteine auf dem Friedhof von Alyscamps in Arles. Albert Dauzat leitet im „Dictionnaire étymologique de la langue

française“ die Silbe „alys“ aus dem gallischen Wort „alisia“ ab, das in zahlreichen Ortsnamen vorkommt und in das spanische Wort für Erle – aliso – eingegangen ist.

Die Legende vom männlichen Erlen- und Elfenkönig überliefert daher eine nur noch schemenhafte Erinnerung an eine uralte weibliche weiße und dreifaltige Todesgöttin, die ursprünglich im alten Griechenland beheimatet war und deren Kult über Spanien nach England wanderte, wo Alphito alias Cerridwen ihr Geschlecht wechselte und zu Bran wurde.

Der Mythos berichtet korrekt, dass Bran Kinder in die andere Welt entführt – wie sein Alter Ego Erlkönig. Dass der Erlkönig in Wahrheit eine Frau ist und warum sie Krone und Schweif trägt wie in Goethes Gedicht, weiß auch die jüdische Mythologie. Die griechische Göttin Alphito ist viel älter – und kleine Jungen gestohlen hat sie schon immer. In Wahrheit verbirgt sich hinter Alphito Lilith, nach dem Talmud die erste Frau Adams. Lilith wurde verstoßen, weil sie sich weigerte, Adam zu gehorchen. Weil sie nicht ins Paradies zurückkehren wollte, befahl Jahwe drei Engeln, täglich einhundert ihrer Kinder zu töten. Und deshalb stiehlt sie immer noch neugeborene Babys. Die Göttin hat sich in einen weiblichen Nachtdämon verwandelt. Von Lilith ist der rachedurstige Satz überliefert:

„Know ye not that I have been created for the purpose of weakening and punishing little children, infants and babes. I have power over them from the day they are born until they are eight days old if they are boys.“

Lilith habe in der Volksmythologie lange, wirr abstehende Haare und Flügel, berichtet die altehrwürdige Encyclopaedia Judaica. Abbildungen von Lilith, die das beweisen (vgl. Fotos), sind schon aus babylonischer Zeit bekannt.

In Deutschland gibt es nur ein Zeugnis von Lilith. Der jüdische Friedhof in Grebenau am Vogelsberg zeigt ein

geflügeltes Wesen mit Menschengesicht. Es handelt sich nicht um den Engel Rasiel, wie dort behauptet wird, sondern um Lilith, deren zweiter Name Meyalleleth im Buch „Sefer Rasiel„, einer rabbinischen Überlieferung, erwähnt wird. Dort werden auch die Formeln beschrieben, die Amulette enthalten müssen, um Neugeborene vor der Dämonin zu schützen. Die Krone und der Schweif des Erlkönigs sind eine volkstümliche ikonografische Verballhornung der Haare und der Flügel Liliths.

Das Computerspiel Blade kennt den Charakter „Lilith Meyalleleth“. So transportiert nicht nur Literatur, sondern auch moderne Spielkultur im Internet uralte Mythen. Man hätte Recht, wenn man „Lilith Meyalleleth“ die „Erlkönigin“ nennen würde.

[English abstract: „German Myth 9 – Goethe and the “Erlkönig” Mistranslation“]

Security by obscurity im Bundestag

Der Bundestag bietet an, den Abgeordneten verschlüsselte E-Mails senden zu können. Das hört sich gut an, funktioniert aber nicht: Kaum ein Abgeordnetenbüro weiß damit umzugehen. Bei technischen Fragen geht man zudem nach dem Motto vor: Security by obscurity.

Die rot-grüne Bundesregierung hat am 22. Januar 2002 die Telekommunikations-Überwachungsverordnung (TKÜV) erlassen. Seitdem wird die Kommunikation aller Bundesbürger komplett überwacht. Die Technik – eine Echtzeit-Schnittstelle – muss von den Telekommunikationsanbietern eingerichtet und selbst finanziert werden. Nur kleine Provider sind davon ausgenommen.

Wer seine elektronische Kommunikation verschlüsselt, kann natürlich nicht belauscht werden. Was liegt also näher, auch bei vertraulichen Nachrichten an einen Abgeordneten des Bundestages kryptografische Verfahren zu verwenden.

Es scheint zunächst einfach zu sein: Unter der Überschrift „Senden verschlüsselter E-Mails an Mitglieder oder Mitarbeiter des Deutschen Bundestages“ kann sich jeder über die Grundlagen asymmetrischer Kryptografie informieren. Man wird auch hinreichend über die Methode aufgeklärt:

„Für die Verschlüsselung von E-Mails muss der jeweilige Absender den öffentlichen Schlüssel des Empfängers in seinen E-Mail Client einbinden. Der öffentliche Schlüssel für die jeweilige E-Mail Adresse der Abgeordneten und Verwaltungsmitarbeiter ist automatisch in jeder signierten E-Mail des Abgeordneten oder Mitarbeiters enthalten. Gegebenenfalls bitten Sie Ihren Kommunikationspartner im Deutschen Bundestag Ihnen eine signierte E-Mail zu senden, um ihm verschlüsselt antworten zu können.“

Vor das Verschlüsseln hat die Verwaltung des Bundestags eine hohe Hürde gestellt: Die E-Mail-Adressen, die man benötigt, um seinen eigenen öffentlichen Schlüssel an die Abgeordneten zu senden, werden nicht verraten, sondern stattdessen jeweils ein Kontaktformular angeboten. Viele Abgeordnete haben zwar eine Website, die muss man aber in jedem Fall einzeln und mühsam selbst recherchieren. Ob das zu erwartende System vorname.nachname@bundestag.de funktioniert, erfährt man auch nicht.

Selbst bei Jörg Tauss (SPD), der bei Internet-Themen als relativ kompetent gilt, ist von einem öffentlichen Schlüssel nichts zu sehen. (Dafür begegnet man aber auf seiner Website dem „Regenzauber“, gegen Spam das @ verklausuliert (a) zu schreiben, wodurch man gezwungen ist, die E-Mail-Adresse mühsam von Hand einzutippen, statt im Quellcode zum Beispiel schlicht Unicode zu benutzen, um es den Spambots nicht ganz so einfach zu machen)

Man muss also zuerst die real existierende E-Mail-Adresse erfragen, auf eine signierte Antwort hoffen, das Zertifikat des Bundestags in den eigenen E-Mail-Client implementieren, die Signatur der empfangenen E-Mail überprüfen, den darin enthaltenen Schlüssel einbinden, dann mit einem eigenen Zertifikat signieren und mit dem öffentlichen Schlüssel des Abgeordneten verschlüsseln – und hoffen, dass der Empfänger die gleiche Methode anwendet und dann endlich auch verschlüsselt schreiben kann.

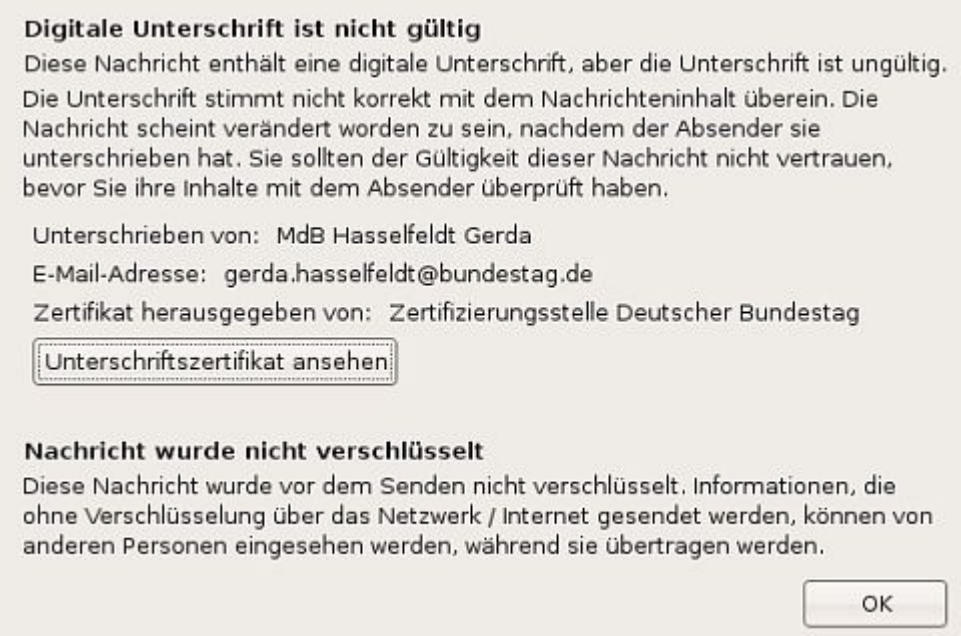
Der Bundestag verwendet nicht die Open-Source-Methode GNU Privacy Guard (GnuPG) oder gar die kommerzielle Version Pretty Good Privacy (PGp) wie etwa das Bundesverfassungsgericht,

sondern verschlüsselt über Secure/Multipurpose Internet Mail Extensions (S/MIME).

Diese Methode hat ihre Tücken: Benutzerfreundlich ist sie nicht, denn kaum ein Computer-Laie wird wissen, wie er oder sie an ein S/Mime-Zertifikat kommen kann und wie das anzustellen sei. Außerdem vertragen sich bei den meisten gängigen E-Mail-Programmen die beiden Verschlüsselungs-Methoden nicht. Thunderbird zum Beispiel arbeitet zuerst die S/Mime-Routinen ab, dann GnuPG. Wenn man eine E-Mail mit S/Mime signiert, kann man GnuPG nicht parallel verwenden, da eine anschließende Verschlüsselung die Mail verändern würde und die Signatur ungültig wäre. Es gibt auch keine Möglichkeit, für bestimmte Empfänger festzulegen, welche S/MIME-Funktion angewendet werden soll. Es ist also immer mühsame Handarbeit angesagt. Das weiß offenbar auch die Pressestelle des Bundestags, die auf Anfrage dazu etwas vage antwortet: „Der Deutsche Bundestag hat sich nur für eine der beiden Alternativen entschieden, da die parallele Verwendung zu technischen und organisatorischen Problemen führen könnte." Der Bundestag hat das zusätzliche Problem, dass er nur eine deutsche Zertifizierungsinstanz benutzen kann. Er ist zwar Certification Authority, kann aber das – auch aus Kostengründen – nicht in gängige Browser und Mail-User-Agenten implementieren lassen.

Am 19. Januar wurden 46 (von 613) nach dem Zufallsprinzip ausgewählte Abgeordnete angeschrieben mit der Bitte: „Bitte schicken Sie mir eine signierte E-Mail zu." Nach einer Woche (!) hatten nur sieben geantwortet, von dem angeschriebenen Abgeordneten der Partei „Die Linke" reagierte sogar niemand. Das Büro von Michael Glos (CSU) war mit am schnellsten: Man wusste offenbar sofort, worum es ging, jedoch fehlte die Signatur. Dafür erfährt man immerhin bei jeder Antwort die eigene IP-Adresse, die man beim Abschicken der E-Mail verwendet hatte – warum auch immer: „Diese Nachricht wurde im Internet des Deutschen Bundestages erfasst – Sa Jan 19

18:03:31 2008 – Externe IP-Adresse: 217.83.70.227.“ Auf Nachfrage reagierte Glos‘ Büro dann nicht mehr.



Eine Mitarbeiterin Volkmar Vogels (CDU) rief sogar an, um sich erklären zu lassen, um welchen unverständlichen Sachverhalt es sich in der fraglichen E-Mail gehandelt habe. Danach scheint das Interesse am Thema aber erloschen zu sein – eine elektronische Antwort kam nicht. Auch das Büro des Bundesinnenministers Wolfgang Schäuble (CDU) schwieg eisern. Zugunsten Schäubles muss erwähnt werden, dass die Standard-Signatur des Autors vermutlich sehr abschreckend wirkt: „Please note that according to the German law on data retention, information on every electronic information exchange with me is retained for a period of six months.“

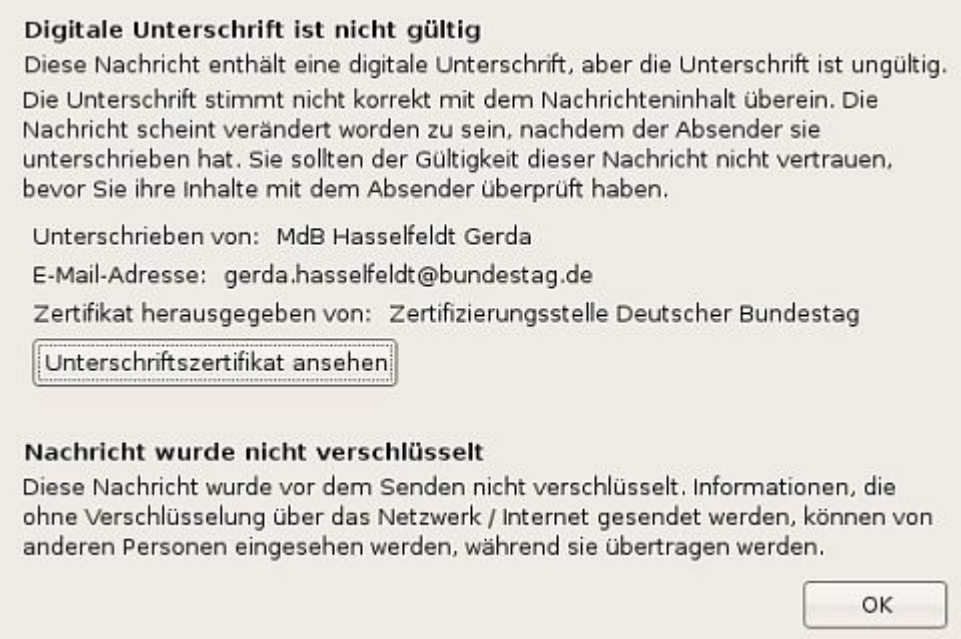
Gerda Hasselfeldt, CDU/CSU, Petra Bierwirth (SPD), Lydia Westrich (SPD) und Miriam Gruß (FDP) antworteten kurzfristig und korrekt signiert, jedoch nur zwei Männer: Markus Löning (FDP) und Hans-Christian Ströbele (Die Grünen). Das Büro Ströbeles, das offenbar zusätzlich die EDV im Bundestag bemühte, kommentierte: „Leider mussten die Techniker einräumen, dass das System noch nicht wirklich gut funktioniert.“ Nur sieben von 47 Mitgliedern des Bundestages reagieren also auf eine E-Mail, die um das bittet, was der Bundestag selbst empfiehlt – eine traurige Bilanz.

Der zweite Schritt gab auch den wenigen Abgeordneten, deren Mitarbeiter verstanden hatten, was eine elektronische Signatur ist, große Rätsel auf:
„Um nachzuprüfen, ob nicht nur die elektronische Signatur, sondern auch die Verschlüsselung funktioniert, bitte ich Sie um eine weitere kurze Mail, die Sie bitte an mich verschlüsseln. Mein öffentlicher Schlüssel (S/Mime) ist in meiner Signatur enthalten."

Nur zwei Abgeordnete – Lydia Westrich und Markus Löning – meisterten diese Hürde und antworteten per verschlüsselter E-Mail. Das Büro von Miriam Gruß gab sich Mühe und kündigte an, man werde sich im Haus sachkundig machen – was aber seitdem offenbar noch nicht von Erfolg gekrönt war. Ein Verantwortlicher für die Technik im Bundestag verriet per verschlüsselter E-Mail, dass es für Probleme dieser Art sogar eine telefonische Hotline gebe und jederzeit Hilfe, falls ein Abgeordneter darum bäte.

Welche technischen Probleme Mitglieder des Bundestag daran hindern könnten, ihre Kommunikation zu verschlüsseln, war nicht zu erfahren. Einige Signaturen wiesen darauf hin, dass die Unterschrift ungültig sei. Das wird vermutlich daran liegen, dass verschlüsselte E-Mails an Bundestagsabgeordnete von einem zentralen Server entschlüsselt werden – ein Prinzip, dass der Idee widerspräche, dass nur der Empfänger einer kodierten Nachricht diese auch lesen sollte. Wie die Sicherheit der Kommunikation zwischen dem Server des Bundestags und Empfänger gewährleistet sei, darüber wollte man keine Details preisgeben. Anna Rubinowicz-Gründler, Pressereferentin im Bundestag, antwortete: „Zu IT-sicherheitsrelevanten Fragen können wir keine Auskünfte erteilen." Auf die Frage, warum ein Kontaktformular, das Signieren und den Austausch von Schlüsseln per S/MIME nicht erlaubt, angeboten wird statt einer funktionierenden E-Mail-Adresse, verwies man darauf, dass „die in das Formular eingetragenen Daten (..) verschlüsselt über ‚HTTPS'

übertragen“ werden. Das bedeutet in diesem Fall nichts, da offenbar niemand genau weiß, wer im Bundestag die Mails welcher Abgeordneten lesen kann. Die mangelnde Fähigkeit oder Bereitschaft der Abgeordneten, ihre E-Mails vor dem Zugriff anderer zu schützen zu wollen, mochte man ebenfalls nicht kommentieren: „Die Pressestelle des Deutschen Bundestages informiert über Sachverhalte, transportiert aber keine Meinungen.“



Über diesen Sachverhalt kann man geteilter Meinung sein. Dass ein Abgeordneter des Bundestages keinen technischen Sachverstand besitzt, ist verzeihlich. Dass sie oder er auf auf den Sachverstand verzichtet, der ihm innerhalb des Hauses gratis angeboten wird, ist einfach nur ignorant.

Dieser Artikel erscheint leicht verändert am 04.02.2008 auf Telepolis.

Operation Heisse Luft, revisited

Schon merkwürdig, dass in dem Heise-Artikel „Kinderporno: Wie erfolgreich war die Operation „Himmel“?“ mit keinem Wort oder Link mein Artikel bei Telepolis „Operation Heiße Luft“ erwähnt wird. Autor ist der c’t-Reakteur Volker Briegleb.

Virtuelles Geld, reale Banken – und umgekehrt

Ein Artikel von mir in der Netzeitung (08.02.2008): „Virtuelles Geld, reale Banken – und umgekehrt“ – „Wenn die Weltwirtschaft wie derzeit durch die US-Immobilienkrise erschüttert wird, leidet dann auch die virtuelle Wirtschaft?“ [mehr…]

Grosser Online-Lauschangriff, revisited

Meine Gattin Claudia weist mich zu Recht darauf hin, dass ich ihre juristische Argumentation zum Thema „großer Online-Lauschangriff“ übernommen habe. Aber sicher. Sie sagt:

> *Der entscheidende Unterschied zwischen der Argumentation Buermeyers und der meinen: Buermeyer stellt klar, daß mit*

> *technischen Maßnahmen und formalgesetzlich sicher zu stellen ist, daß kernbereichsrelevante Daten geschützt bleiben. Eine darüber hinausgehende Schlußfolgerung ist, daß solange diese technischen Maßnahmen nicht vorhanden sind, die Online-Durchsuchung in jedweder Form mit der derzeitigen Rspr. des BverfG zum Kernbereichsschutz nicht in Einklang zu bringen ist.*

Meine Gattin hat natürlich Recht.

Security by obscurity im Bundestag

Ein Artikel von mir auf Telepolis (04.02.2008): „Security by obscurity im Bundestag – Über Ahnungslosigkeit, Versagen und S/Mime. Der Bundestag [extern] bietet an, den Abgeordneten verschlüsselte E-Mails senden zu können. Das hört sich gut an, funktioniert aber nicht: Kaum ein Abgeordnetenbüro weiß damit umzugehen. Bei technischen Fragen geht man zudem nach dem Motto vor: Security by obscurity.“ [mehr…]

Grosser Online-Lauschangriff?

Die aktuellen juristischen Gutachten zur „Online-Durchsuchung“ sind sich in zwei Fragen einig: Technisch ist sie kaum machbar, und gegen sie sprechen schwer wiegende verfassungsrechtliche Bedenken. Das Bundesinnenministerium

ficht das nicht an. Dessen Informationspolitik kann auch zu dem Fazit führen, dass die die Öffentlichkeit – wider besseres Wissen der Verantwortlichen – getäuscht werden soll.

Der Dritte Strafsenat des Bundesgerichtshofs hat schon vor einem knappen Jahr die „verdeckte Online-Durchsuchung“ verboten. In Kürze wird entschieden, ob die Verfassungsbeschwerde gegen deren bisher einzige juristische Ermächtigungsgrundlage, das nordrhein-westfälische Verfassungsschutzgesetz, Erfolg haben wird. Das Bundesverfassungsgericht wird über die so genannte „Online-Durchsuchung? jedoch nur indirekt urteilen. Im fraglichen Gesetz heißt es wörtlich, es gehe um „heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel.“ Der Begriff „Online-Durchsuchung? kommt im Text gar nicht vor. Die Idee, die Strafverfolger und die Behörden würden auf privaten Rechnern heimlich Software installieren können, ist eine Erfindung der Medien, insbesondere der Süddeutschen (07.12.2006) und der taz (30.01.2007). Der polizeiliche „Hackerangriff“ hat sich jedoch im allgemeinen Sprachgebrauch und seit dem Medienhype vor einem Jahr auch als Wunschvorstellung in der Politik eingebürgert.

Ulf Buermeyer, wissenschaftlicher Mitarbeiter beim Bundesverfassungsgericht, hat im August 2007 in einem Aufsatz umrissen, warum schon aus der vergangenen Rechtsprechung abgeleitet werden kann, dass ein heimlicher Zugriff des Staates auf private Rechner, wie von Schäuble befürwortet, schlicht verfassungswidrig ist. Unter „Zugriff? kann man verstehen, mit Hilfe technischer Mittel den Rechner eines Verdächtigen – ohne dessen Wissen – über einen bestimmten Zeitraum zu überwachen, auch ohne dass die dazu notwendige Software „online? implementiert werden müsste. Das ist ohnehin noch nie erfolgreich geschehen, trotz gegenteiliger Meldungen

in den Medien, und auch äußerst unwahrscheinlich, da sich jeder dagegen mit einfachen Mitteln schützen könnte.

Buermeyer zweifelt in seinem Text „Die „Online-Durchsuchung“. Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme? nicht nur daran, dass die Ermittlungsmethode der Online-Durchsuchung „jemals effektiv wird angewendet werden können?, sondern führt zwei gewichtige juristische Argumente an, die das Bundesverfassungsgericht zu erwägen habe – die Unverletzlichkeit der Wohnung nach Artikel 13 Absatz 1 des Grundgesetzes und den so genannten „Kernbereichsschutz“ privater Lebensgestaltung. Interessant ist der Aufsatz Buermeyers vor allem deshalb, weil er beweist, dass das Bundesverfassungsgericht seine bisherige Rechtsprechung über den Haufen werfen müsste, erlaubte es das, was dem Bundesinnenministerium vorschwebt (zum Beispiel in den „Fragen und Antworten zur Online-Durchsuchung“.

Das Bundesverfassungsgericht hat am 3. März 2004 zum „Großen Lauschangriff“ geurteilt, das Grundrecht auf Unverletzlichkeit der Wohnung meine nicht nur den Schutz vor unerwünschter physischer Anwesenheit eines Vertreters der Staatsgewalt in allen Räumen, die privat und beruflich genutzt werden – inklusive Keller, Balkon und Garten, ja sogar ein zeitweilig genutztes Hotelzimmer. Es ging noch viel weiter:

> *„Die heutigen technischen Gegebenheiten erlauben es, in die räumliche Sphäre auch auf andere Weise einzudringen. Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes1 umfasst wäre.“*

Die wenigen Juristen, die eine heimliche „Online-Durchsuchung“ für unbedenklich halten, kommen um diese Argumentation des Bundesverfassungsgerichts nicht herum. Die Wohnung ist sakrosankt, und was das Bundesverfassungsgericht einmal entschieden hat, besitzt quasi Gesetzeskraft. Man kann das nur durch verbale Taschenspielertricks umgehen. Einige Juristen konstruieren um den Computer einen „virtuellen Raum?, der mit einem Online-Anschluss entstehe und der daher nicht mehr zur „Wohnung? gehöre (*vgl. Beulke/Meininghaus: „Anmerkung zur Entscheidung des BGH vom 21.2.2006 StV 2007, S. 63*). Noch abwegiger ist zum Beispiel die These, derjenige, der sich des Internet bediene, wüsste, dass sein Computer „hierdurch vielfältigen Angriffen durch Würmer usw.“ ausgesetzt sei. Der Nutzer nehme das somit in Kauf, öffne sein System selbst und begebe sich damit in die „Sozialsphäre?, die keine „Wohnung? mehr sei. Dr. Jürgen P. Graf, damals Oberstaatsanwalt beim Bundesgerichtshof, meinte noch 1999 in der Deutschen Richterzeitung, der Anbieter von Daten erkläre sich mit der Eröffnung des freien Zugangs im Internet „mit dem Zugriff durch beliebige Dritte? automatisch einverstanden. Mit dem technischen Sachverstand der meisten Juristen ist es ohnehin

nicht sehr weit her. Die überwiegende Anzahl der Autoren nimmt es unkritisch als Tatsache hin, dass ein – wie auch immer gearteter – „Bundestrojaner“ technisch umsetzbar sei. Man könnte auf ähnlichem Niveau auch darüber diskutieren, ob der Einsatz einer Tarnkappe – wie im Nibelungenlied – für Polizisten der Verfassung entspräche.

Buermeyer aber war Netzwerk-Administrator der Universität Leipzig und ist daher eine Ausnahme. Die zweite Säule seiner Argumentation, warum eine Online-Durchsuchung verwassungswidrig sei, ist der Schutz des Kernbereichs privater Lebensgestaltung. Der fußt auf der durch den Artikel 1 des Grundgesetzes geschützten unantastbaren Menschenwürde. Noch nicht einmal der Bundestag könnte diesen Artikel mehrheitlich abschaffen oder verändern:

> *„Aus der Menschenwürdegarantie folgt nach der Rechtsprechung des Bundesverfassungsgerichts zwar nicht, dass ein heimliches Vorgehen des Staates schlechthin unzulässig wäre, denn allein darin, dass der Mensch zum Objekt der Beobachtung wird, ist noch nicht zwingend eine Missachtung seines Wertes als Mensch zu erblicken. Gleichwohl ist bei staatlichen Beobachtungen ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren, denn würde der Staat in ihn eindringen, verletzte dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen. Insbesondere ist kein Raum für eine Abwägung mit kollidierenden Rechtsgütern wie dem staatlichen Strafverfolgungsinteresse.“*

In diesem „Kernbereich? darf der Staat noch nicht einmal Daten erheben. Das hat das Bundesverfassungsgericht eindeutig formuliert und damit auch allen Ideen eines „Richterbands“ oder „Richtervorbehalts? eine Absage erteilt. Für die Online-

Durchsuchung heißt das: Da es keine technischen Möglichkeit gibt, auf einem Rechner vorab „private“ Daten, die unter diesen „Kernbereich“ fallen, von denen zu trennen, für die das eventuell nicht zutrifft, verbietet sich der Einsatz heimlicher staatlicher Schnüffel-Software sogar bei Keyloggern.

Das Bundesinnenministerium müsste genug sachverständige Experten haben, die sowohl die juristische Argumentation als auch die technischen Implikationen nachvollziehen könnten. In den „Fragen und Antworten zur Online-Durchsuchung“, die mittlerweile auch auf der Website des Bundeskriminalamts verlinkt ist, wird jedoch das Gegenteil suggeriert. Auf das Urteil des Bundesgerichtshofs gegen die Online-Durchsuchung wird mit keinem Wort eingegangen, bloße technische Spekulationen werden für bare Münze ausgegeben:

> *„Bevor eine Online-Durchsuchung durch Beamte des Bundeskriminalamts (BKA) durchgeführt wird, prüft ein unabhängiger Richter grundsätzlich, ob diese Durchsuchung auf einem PC einer Privatperson oder in einer Firma durchgeführt werden darf.“ (…) Die Ermittlungs-Software wird nicht zu einer Beeinträchtigung der auf dem betroffenen Rechner installierten Sicherheitssoftware führen. (…) Sollte die*

> *Software dennoch entdeckt werden, wird sie vom Zielsystem entfernt.“*

Diese drei Thesen haben weder eine rechtliche Grundlage noch sind sie als unverbindliche Idee gekennzeichnet. Technisch erscheinen sie ohnehin als unsinnig. Eine derartige Software – inklusive einer Art Selbstzerstörungsmechnismus und der Möglichkeit, gerichtfeste Daten zu bekommen – gibt es noch nicht und wird es wohl auch nicht geben. Das Gutachten Prof. Ulrich Siebers zum Beispiel bekräftigt das differenziert: „Nach den Standards für digitale Forensik ist die Analyse eines im Betrieb befindlichen Systems problematisch, da ständig Daten verändert werden.“ Falls die Daten einen dümmsten anzunehmenden Kriminellen „online“ zu den Strafverfolgern gelangten, hätte die Staatsanwaltschaft größte Probleme, deren Authentizität zu beweisen.

Das Bundesinnenministerium verweigert über den technischen Hintergrund jede Auskunft. Auch auf einfache Fragen erhält man keine Anwort, zum Beispiel:

„Ist Ihnen bekannt, dass sich jeder Computer-Nutzer leicht dagegen schützen kann, dass ihm unbemerkt Fremdsoftware auf den Rechner „gespielt“ wird, wenn man sich an die Ratschläge des Bundesamtes für Sicherheit in der Informationstechnik hält? Wie kann verhindert werden, dass Terroristen die Ratschläge des BSI zum Thema Internet-Sicherheit beherzigen? Ist ihnen bekannt, dass bis jetzt in Deutschland noch kein erfolgreicher Versuch seitens des Bundeskriminalamtes und des Verfassungsschutzes (nach dessen eigenen Angaben) stattgefunden hat, einem Verdächtigen ohne dessen Wissen eine Software auf den Rechner zu spielen, um einen so genannten Remote-Access-Zugang zu erhalten? Haben Sie vor der Veröffentlichung „Fragen und Antworten zum Thema Online-Durchsuchungen“ den Rat Sachverständiger eingeholt, ob eine Online-Durchsuchung überhaupt technisch umsetzbar sei? Was veranlasst Sie zu der Annahme, das sei zukünftig der Fall?

Markus Beyer, Pressereferat des Bundesinnenmministeriums antwortet nur:

> *„Wie Sie wissen handelt es sich bei der geplanten sog. Onlinedurchsuchung, wie auch bei der geplanten Novelle des BKA-Gesetzes insgesamt, um einen laufenden Gesetzgebungsprozess auf Fachebene, der noch nicht abgeschlossen ist. Daher bitten wir um Verständnis, dass wir auf weitere Detailfragen derzeit nicht eingehen können. (…) Insbesondere darf ich darauf hinweisen, dass das Bundesverfassungsgericht allein über eine Regelung des Landes NRW (!) entscheidet. Die geplante Novelle des BKA-G ist nicht Gegenstand der Verhandlung beim Bundesverfassungsgericht.“*

Man tut also so, als ob das möglich sei. Und da das Bundesverfassungsgericht nur über das Verfassungsschutzgesetz eines Bundeslandes befinden will, macht man einfach so weiter, als gebe es die vergangene und aktuelle Rechtsprechung gar nicht. Der Verdacht drängt sich auf, dass man in Schäubles Haus schlicht keine Ahnung hat, wie man das gewünschte polizeiliche „Hacken? bewerkstelligen will. Nur völlig unerfahrene Computer-Nutzer sind durch die wolkigen Formulierungen zu beeindrucken, Terroristen vermutlich nicht.

Auch der bayerische Innenminister Joachim Herrmann forderte in einem
Interview „Online-Durchsuchungen“. Herrmann ist ebenfalls nicht in der Lage, auf nur eine der ihm gestellten Fragen substanziell zu antworten – weder auf die juristischen noch auf die technischen. Zum Beispiel:

„Auf Grund welcher Annahmen geht Herr Joachim Herrmann davon aus, dass es Zukunft eine funktionsfähige Methode zur „Online-Durchsuchung‘ privater Rechner geben wird?“

Oder: „Das Bundesverfassungsgericht hat in einer Entscheidung zum Niedersächsischen Polizeigesetz seine Feststellungen aus dem Jahre 2004 zum Schutz des Kernbereichs privater

Lebensgestaltung vor Eingriffen des Staates nochmals verdeutlicht. Das Gericht hebt hervor, ein Erhebungsverbot bestehe, wenn in einem konkreten Fall Anhaltspunkte vorliegen, dass eine Überwachungsmaßnahme Inhalte erfassen könne, die zu dem definierten Kernbereich gehören. Frage: Wie kann der Schutz des Kernbereichs privater Lebensgestaltung garantiert werden, wenn eine Software auf dem Rechner des Verdächtigen ohne dessen Wissen installiert worden ist?“

Die lapidare Antwort – per Word-Attachment – von Karl Michael Scheufele, dem Pressesprecher des Bayerischen Staatsministeriums des Innern: „Moderne Kommunikationstechnik darf nicht die Folge haben, dass Terroristen rechtsfreie Räume für Verbrechensplanung haben. Wenn solche Organisationen sich dieser Kommunikationsmittel bedienen, dann müssen die Sicherheitsbehörden die Möglichkeiten haben, darauf zu reagieren. Selbstverständlich werden die verfassungsrechtlichen Vorgaben des BverfG eingehalten.“

Man darf getrost annehmen, dass hier der Wunsch der Vater des

Gedankens ist. Aber die Leitmedien argumentierten beim Thema auch nicht gehaltvoller als die Politiker. Auf der Website der Tagesschau wird seit Monaten eine Infografik präsentiert, die suggeriert, eine Online-Durchsuchung würde im Sinne Schäubles schlicht funktionieren, ohne die skeptischen Einwände der IT-Fachleute auch nur ansatzweise zu berücksichtigen. Der Redaktion von tagesschau.de gelang es im Lauf einer Woche nicht, trotz mehrmaliger Anrufe und einiger E-Mails, den zu benennen, der die Infografik erstellt hatte.

„Ist tagesschau.de bekannt, dass es bis jetzt noch keine einzige erfolgreiche Online-Durchsuchung gegeben hat? Was veranlasst tagesschau.de anzunehmen, dass die in der Info-Grafik vorgestellten „Methoden" umsetzbar und praktikabel seien?"

Auch darauf gab es keine Antwort. Was zu beweisen war.

Dieser Artikel erschien leicht gekürzt am 28.01.2008 in Telepolis. Fotomontagen: Burks mit Material des Bundestags und der Tagesschau.

Großer Online-Lauschangriff

Ein Artikel von mir auf Telepolis: „Großer Online-Lauschangriff? – Die aktuellen juristischen Gutachten zur „Online-Durchsuchung" sind sich in zwei Fragen einig: Technisch ist sie kaum machbar, und gegen sie sprechen schwer wiegende verfassungsrechtliche Bedenken". [mehr…]

Drill für Dumpfbacken!

Ein Artikel von mir in der Jungle World (17.01.2008): „Drill für Dumpfbacken! – Wann immer Einwanderer bei einer Debatte in Deutschland eine Rolle spielen, setzt sich der rassistische Konsens durch. Das zeigt die gegenwärtige Diskussion um gewalttätige Jugendliche.“ [mehr…]

Leider ist der Schluss gestrichen worden. Er lautete: „Auf einen groben Koch gehört ein grober Keil, sagt der Volksmund. Leider reagiert die Linke, wer auch immer das sei, nur mit Klagen und Jammern, statt selbst Forderungen aufzustellen, über die die Medien garantiert berichten würden. Der Altmeister der griffigen Parolen, Bertold Brecht, hat dazu schöne Vorlagen geliefert: ‚Es hilft nur Gewalt, wo Gewalt herrscht‘, sagt die Heilige Johanna der Schlachthöfe. Und, etwas frei formuliert, um die Perspektive geradezurücken: ‚Was ist das Verprügeln eines Passanten gegen das Betreiben eines Abschiebeknastes?'“

Die heilige Einfalt der Holzmedien


myFreising Studentencommunity - [Translate this page]
Die heilige Einfalt der Holzmedien · Der Schuster bleibt bei seinen Leisten · Ferngesteuerte Stromversorgung · Spielerlebnis fÃ¼r Hartgesottene · Lausejungs ...
www.myfreising.de/home.html - Similar pages

Nachrichtenkanal der Tageszeitung junge Welt (versalia.de) - [Translate this page]
Die heilige Einfalt der Holzmedien Eine Diskussion zwischen Journalisten und Bloggern offenbart die noch immer existierenden Gräben; Der Schuster bleibt bei ...
www.versalia.de/rss/ - Similar pages

Did you mean to search for: "Die heilige Einfalt der ***Holzmaden***"

Ein Artikel von mir bei Telepolis (13.01.2008): „Die heilige Einfalt der Holzmedien“ – „In Berlin diskutierten Am letzten

Donnerstag Journalisten mit Bloggern. Man redete mit vereinten Kräften aneinander und am Thema vorbei. Die vom Deutschen Journalisten-Verband organisierte Veranstaltung bewies, dass das Internet in den Köpfen der Holzmedien-Vertreter noch nicht angekommen ist. Und viele Blogger wissen nur begrenzt, was Journalismus bedeuten könnte, wie die „Nachbereitung“ der Diskussion zeigt.“ [mehr…]

Toonpool.com: Komik zum Abstimmen

Ein Artikel von mir in der Netzeitung: „Toonpool.com: Komik zum Abstimmen“ – „Die neue Webseite Toonpool.com versammelt deutsche und internationale Cartoons in einer Web 2.0-Atmosphäre. Burkhard Schröder hat sich das Online-Portal einmal genauer angesehen.“ [mehr…]