



Die Operation Payback - kriminelle Handlung oder ziviler Ungehorsam? Ein Einordnungsversuch einer neuen Protestform.

Justus Junghans

1. Einleitung

Ende des Jahres 2010 beherrschte besonders ein Thema die Medien: Die Internetplattform WikiLeaks veröffentlichte tausende als geheim eingestufte Mails von US-Diplomaten, die der Internetseite von unbekannter Stelle aus zugespielt wurden. Ziel von WikiLeaks ist es nach eigenen Angaben "wichtige Nachrichten und Informationen an die Öffentlichkeit zu bringen" (aus dem Englischen von WikiLeaks - About) und damit gewisse Menschenrechte zu stärken. Dies führte zu einer

emotionalen Diskussion in der Öffentlichkeit. Während der laufenden Diskussion kam es ebenfalls dazu, dass große Finanzdienstleister wie die schweizer Bank Postfinance, Mastercard, VISA, PayPal, (vgl. Janssen 2011) das Geschäftsverhältnis mit WikiLeaks kündigten. Da WikiLeaks eine spendenfinanzierte Organisation ist, die ihr Geld über solche Dienstleister einsammelt, schränkte dies die Handlungsfähigkeit der Organisation ein.

Scheinbar erhitzte dies viele Gemüter: Es folgten in den nächsten Tagen digitale Attacken auf die Websites von Unternehmen, die sich Wikileaks gegenüber nicht kooperativ zeigten. Nun könnte man meinen, dass es sich um einen gezielten Angriff einer kleinen, technisch hochversierten Subkultur handle, sogenannter "Hacker". Es scheint jedoch eher so zu sein, dass sich über Soziale Netzwerke wie Twitter spontan eine Bewegung gebildet hat, die ohne großen technischen Aufwand mit einem "extrem einfach zu bedienende[n] Programm" (Janssen et al. 2010) die Firmenauftritte über mehrere Stunden hinweg unzugänglich gemacht hat. Die Aktion lief unter dem Namen "Operation Payback".

Jeder, der teilnehmen wollte, hatte die Möglichkeit, sich eine kleine, kostenlose, schon länger verfügbare Software herunterzuladen und mit wenigen Klicks vor dem eigenen Rechner an dem digitalen Aufstand teilzunehmen. Bei dieser Aktionsform ist der Aufwand für den Teilnehmer gering und benötigt nicht einmal physische Anwesenheit, wie dies bei einer Sitzblockade der Fall ist.

Doch womit haben wir es hier zu tun? Inwieweit ist diese neue Form des Proteste vergleichbar mit bekannten Demonstrationsformen? Und wie gehen wir in unserer Gesellschaft am besten damit um?

Die öffentliche Einordnung dieser Ereignisse ist sehr unterschiedlich. Während die einen von "Hacker-Angriffen" (ZEIT ONLINE 2010) oder "Cyber-Attacken" (ibd.) reden, sprechen andere von "Aktivismus" (Janssen 2011) oder einer "Aktion" (ibd.).

- "Andererseits verteidigte der Politikwissenschaftler und Internet-Theoretiker Evgeny Morozov die Aktion unter Verweis auf 'Eine Theorie der Gerechtigkeit' von John Rawls: DDoS-Angriffe könnten auch eine Form des zivilen Ungehorsams sein." (Janssen 2011)

Ziel dieses Beitrags ist es, zuerst die Handlungen der Angreifer anhand der aktuellen Berichterstattung zu analysieren, inwieweit sie Eigenschaften aufweisen, die sie mit bestehenden Protestformen vergleichbar machen. Danach wird exemplarisch geprüft, ob sich die Operation in Hannah Arendts Ausführungen über zivilen Ungehorsam einordnen lassen und inwiefern es möglich ist, diese Form des Aktivismus mit klassischen Protestformen zu vergleichen. Eine Betrachtung von WikiLeaks und deren Veröffentlichungen selbst wird hier bewusst nicht gemacht.

2. Die Operation Payback

Art der Angriffe

Bei den Angriffen handelt es sich um sogenannte "Distributed Denial of Service - Attacken" (DDoS-Attacken). Hinter dieser Angriffsform steht die Tatsache, dass die Verarbeitung jeder Anfrage, die bei Aufruf einer Website an den die Website speichernden Server gesendet wird, diesen einen geringen Anteil seiner Rechenleistung kostet. Die maximale Rechenleistung eines Servers ist begrenzt. Bei einem DDoS-Angriff werden von verschiedensten Rechnern auf der ganzen Welt (*Distributed*) Anfragen an denselben Server gesendet. Die große Menge der sabotierenden Anfragen beansprucht den Server so sehr, dass er für seinen eigentlichen Zweck (z.B. die Abwicklung von Finanzdiensten über seine Website) keine Rechenleistung mehr übrig hat. Ist die Anzahl der Anfragen groß genug, kann dies also dazu führen, dass eine Website nicht mehr zu erreichen ist; endet der Angriff, ist die Website ohne

Beeinträchtigung wieder zu erreichen. Die Zahl der Anfragen muss über der vom Server verarbeitbaren liegen.

Ziel der Angreifer war es nicht, "die kritischen Infrastrukturen der betroffenen Organisationen zu stören. Vielmehr wolle man ihre Unternehmens-Websites, also ihren Auftritt in der Öffentlichkeit, stören." (Janssen 2011)

Individuelle Handlung

Für eine DDoS-Attacke benötigt man per Definitionem (*Distributed*) eine große Anzahl an verschiedenen Computern, um von verschiedenen Punkten aus Anfragen senden zu können. In der Regel hat eine Einzelperson keinen Zugriff auf eine technische Infrastruktur, die es ermöglicht, einen solchen Angriff alleine durchzuführen.

Um an solch einem Angriff teilzunehmen, waren folgende Handlungen notwendig: Man musste sich im Internet über die Organisation der Angriffe informieren. Dies ist notwendig, um später gleichzeitig das selbe Ziel angreifen zu können. Des weiteren musste man sich das für DDoS-Attacken entwickelte Programm *LOIC* (Low Orbit Ion Cannon; ein Kunstname, der auf ein Computerspiel zurückgeht) auf den eigenen Rechner herunterladen. Mit diesem "extrem einfach zu bedienende[n]" (Janssen et al. 2010) Programm ist es möglich automatisiert eine extrem große Menge Anfragen zu einem zentral koordinierten Zeitpunkt an ein ebenfalls zentral koordiniertes Ziel zu senden.

Es gibt prinzipiell noch andere Möglichkeiten an dem Angriff teilzunehmen. Die einfachste wäre, die Website mit seinem Webbrowser von Hand mehrfach aufzurufen. Der hier beschriebene Weg richtet sich nach dem in der Computerzeitschrift *c't* beschriebenen, der von den AktivistInnen auch verwendet wurde. (vgl. Janssen et al. 2010)

Koordination

Koordiniert wurden die Angriffe durch einen "lose[n] Zusammenschluss anonymer Internetaktivisten" (Janssen 2011), die sich über öffentlich zugängliche Internetdienste koordinieren. Man kann das Programm *LOIC*

so konfigurieren, dass es sich über das Internet von einer zentralen Stelle fernsteuern lässt. Zu dieser Fernsteuerung scheint es eine "Führungsriege" (Janssen et al. 2010) zu geben, die Zugriff auf die fernsteuernden Server hat. Jeder, der LOIC benutzt, musste sich die Information, welche "Befehlsgeber" (ibd.) verwendet werden, selbst suchen und die Konfiguration durchführen.

Ablauf

Im Dezember 2010 waren aufgrund von DDoS-Angriffen mehrere Webseiten für Internetsurfer un erreichbar. Die Webseiten waren "zum Teil tagelang lahm[gelegt]" (Janssen 2011), wie das Computermagazin c't berichtet. Die Angriffe gingen von vielen Teilnehmern gleichzeitig aus:

- "Während das DDoS-Rudel bei der Postfinance-Attacke nur aus knapp 400 Rechnern bestand, waren an den Mastercard-, Visa- und Paypal-Angriffen zeitweise mehrere tausend Computer beteiligt." (Janssen et al. 2010)

Angegriffen wurden die öffentlichen Homepages von Firmen. Dadurch kann ein wirtschaftlicher Schaden entstehen, da für Kunden die Homepage nicht zu erreichen ist. Es könnte auch möglich sein, dass im Zuge der Angriffe das Image der Firmen Schaden nimmt. Konkrete Angaben zu einer Schadenshöhe wurden nicht gefunden. In einer Pressemitteilung der schweizer Postfinance heißt es: "Der Zugriff auf www.postfinance.ch und damit auch auf E-Finance ist im Augenblick durch eine Häufung von Internetanfragen überlastet. Die Sicherheit der Kundendaten ist dabei nicht betroffen" (postfinance.ch 2010), und PayPal veröffentlicht die Mitteilung, dass es neben leichten Verlangsamungen keine wesentlichen Beeinträchtigungen gab (vgl. PayPal | Blog 2010).

Anonymität im Netz

Laut der Berichterstattung in der c't verhält es sich so, "dass Beteiligte an den DDoS-Attacken keineswegs – wie sie vielleicht glauben – in der anonymen Masse untergehen." (Janssen 2011) Durch die Protokollierung der IP-Adressen auf den Servern ist die Rückverfolgung für die Strafbehörden möglich. Dies zeigen auch die Verhaftungen, die in einigen Ländern den Angriffen folgten. (vgl. ZEIT ONLINE 2010)

3. Straftat oder ziviler Ungehorsam?

Hannah Arendt hat sich ausführlich mit politischen und gesellschaftlichen Theorien auseinandergesetzt. In den siebziger Jahren, die in Amerika von den großen Protesten gegen den Vietnamkrieg geprägt waren, beschäftigte sie sich ausführlich mit dem Phänomen des zivilen Ungehorsams. In einem Aufsatz, der aus einem 1970 gehaltenen Vortrag auf einem New Yorker Kongress zum Thema "Is law dead?" hervorging, beschreibt Arendt ausführlich, auf Grundlage der amerikanischen Gesetzeslage und Landesgeschichte, was unter dem Begriff *ziviler Ungehorsam* zu verstehen ist, und formuliert auch, wie wir mit zivilem Ungehorsam gesellschaftlich umgehen können. (vgl. Arendt 2000: 463) Es handelt sich hierbei um keine allgemeine Einführung in eine Grundsatztheorie, sondern um eine praktische Anwendung moral- und gesellschaftsphilosophischer Thesen.

Das Interesse am eigenen Selbst

Der Aufsatz ist nach der Einleitung in drei Abschnitte unterteilt. Im ersten werden die beiden bedeutenden historischen Fälle von Sokrates und Thoreau betrachtet. Beiden ist gemeinsam, dass sie aus Gründen ihrer persönlichen Moral eine bestimmte, staatlich geforderte Handlung nicht durchführen wollten, und beide dafür bestraft wurden. Diese Strafe wurde dabei auch ohne Beschwerde in Kauf genommen, obwohl sie Thoreau die Freiheit und Sokrates sogar das Leben kostete. Hannah Arendt arbeitet heraus, dass es einen klaren Unterschied zwischen der moralischen Ebene und der Ebene der Legalität, des Rechtes gibt. Auch wenn beide aus Gewissensgründen eine bestimmte Handlung

verweigern, stellen sie nicht das Gesetz an sich in Frage. Die moralische Notwendigkeit für die beiden, das Gesetz zu brechen und damit eine Strafe in Kauf zu nehmen begründet Arendt im "Interesse am eigenen Selbst" (Arendt 2000: 292):

- "Diese Vorschriften bedeuten dem Menschen: Hüte dich davor, etwas zu tun, mit dem du dann nicht leben kannst." (Arendt 2000: 292)

Dieser Satz spiegelt den Kern von Hannah Arendts Handlungsethik wieder. (vgl. Martens 2000: 245) Jeder Mensch soll so handeln, dass er sein Leben lang persönlich mit seinen Entscheidungen - auf der Basis seines Gewissens - leben kann.

In Bezug auf die Teilnahme an der *Operation Payback* bedeutet dies, dass ein Teilnehmer der Attacken, bevor er die LOIC-Software anwendet (was vielleicht gegen geltendes Recht verstößt oder auch durch den geplanten Schaden, den die Aktion anrichten soll, gegen gesellschaftlich-moralische Normen) prüfen muss, ob er mit dieser Entscheidung sein Leben lang mit seinem Gewissen leben kann. Arendt erkennt in dieser Basis der Entscheidungsfindung zwei Probleme: Das Gewissen ist rein subjektiv und es setzt voraus, dass sich der Mensch damit auch auseinandersetzt. (vgl. Arendt 2000: 292) Individuell muss sich ein Mensch mit seinem Gewissen auseinandersetzen, um die richtige Entscheidung zu treffen. Im von Hannah Arendt beschriebenen Fall der amerikanischen Proteste lag eine rechtliche Grauzone vor. Die Teilnehmer konnten bestraft werden, da sie an einer nicht legalen Versammlung teilnahmen, konnten sich aber auch auf höhere Gesetze berufen, wie zum Beispiel auf die Freiheit der Meinungsäußerung. In diesem Fall muss ein Richter im Namen der Gesellschaft eine Abwägung treffen und entscheiden, welche Schuld den Gesetzesbrecher tatsächlich trifft. Arendt untersucht, ob man die Handlungen als kriminell bezeichnen muss, oder ob man sie in eine zweite Kategorie einordnen kann - die des zivilen Ungehorsams.

Ziviler Ungehorsam

Im zweiten Abschnitt wird diese Abgrenzung genau gezogen. Juristisch gesehen "wird das Gesetz dadurch um nichts weniger verletzt, als daß es in einem Akt zivilen Ungehorsams gebrochen wird und nicht durch ein

kriminelles Vergehen." (Arendt 2000: 298) Arendt sieht den zivilen Ungehorsam klar getrennt von einem Verbrechen.

Als erstes und wichtigstes Wesensmerkmal ist der zivile Ungehorsam immer an eine Gruppe, die sich durch eine gemeinsame Meinung auszeichnet, gebunden. In den meisten Fällen stellt diese eine Minderheit dar.

- "Ziviler Ungehorsam entsteht, wenn eine bedeutende Anzahl von Staatsbürgern zu der Überzeugung gelangt ist, daß entweder die herkömmlichen Wege der Veränderung nicht mehr offen stehen beziehungsweise auf Beschwerden nicht gehört und eingegangen wird [...]" (Arendt 2000: 299)

Damit ist auch verbunden, dass man im zivilen Ungehorsam öffentlich handelt und nicht im Verborgenen. Ein Krimineller handelt "ausschließlich im eigenen Interesse", er entzieht sich der "Gewalt der Vollstreckungsorgane" (Arendt 2000: 300), ein im Sinne des zivilen Ungehorsams Protestierender handelt im Sinne der Gruppe und damit nie alleine und nie im Verborgenen.

Die zweite Eigenschaft des zivilen Ungehorsams ist die Gewaltlosigkeit. (vgl. Arendt 2000: 301)

Nun können wir aufzeigen, wie sich die DDoS-Angriffe in dieser Unterscheidung einordnen lassen: Bei der Teilnehmerzahl von zeitweise mehreren tausend Rechnern können wir davon ausgehen, dass es sich im Sinne Arendts um eine *bedeutende Anzahl* an Personen gehandelt hat. Wenn die Teilnehmer durch das Internet nicht anonym waren, was laut c't der Fall war, haben wir es, auch wenn keine physische Anwesenheit an einem Ort nötig ist, nicht mit einer Handlung im Verborgenen zu tun, da sich die Personen nicht der Strafverfolgung entziehen. Es sei jedoch angemerkt, dass sich die Identität im Internet durch Hilfsmittel durchaus verschleiern lässt, und dass sich damit auch die Einordnung der Handlung ändert.

Die nächste und weitaus schwierigere Frage ist, ob wir es hier mit einer gewaltfreien Handlung zu tun hatten. Gewalt anwenden bedeutet einem Gegenüber durch sein Handeln einen Schaden zufügen. Ein Schaden ist durch die Unerreichbarkeit der betroffenen Websites zweifelsfrei

entstanden. Unbeteiligte Bürger, die Informationen von der Website abrufen wollten, konnten diese nicht erreichen. Im Rahmen von klassischen "gewaltfreien" Demonstrationen entsteht allerdings auch ein Schaden, beispielsweise durch die Blockade von Gleisen durch Atomkraftgegner bei einem Castortransport.

Die Aktivisten zielen laut c't nur auf Störung der Firmenpräsenz im Internet und nicht auf "[kritische] Infrastruktur" (Janssen et al. 2010) selbst. Ebenfalls sind die Websites nach Beendigung der Attacke wieder voll funktionsfähig. Dies wäre vielleicht vergleichbar mit einer Sitzblockade vor dem Eingang eines Konzerns. Betrachtet man allerdings die Organisation der Aktionen im Internet können Zweifel an der Friedlichkeit aufkommen. Im Internet kursierten Bilder, auf denen die Aktivisten in roter und weißer Schrift auf schwarzem Grund die nächsten Angriffe ankündigten. Diese Bilder wurden über soziale Netzwerke oder über andere Internetdienste weitergereicht, um die Teilnehmer zu koordinieren. Eines dieser Bilder kündigt den nächsten Angriff auf PayPal an:

- "We will fire at anyone or anything that tries to censor WikiLeaks, including multi-billion dollar companies such as PayPal. Twitter, you're next for censoring #wikileaks discussion. The major shitstorm has begun." (N. N. zitiert nach FoxNews.com 2010)

Dies klingt in unseren Ohren eher nach einer Vergeltungsaktion als nach einem Aufruf zum friedlichen Protest. Es wird klar, dass man auch die Gewaltfreiheit der Demonstranten, Angreifer, Aktivisten oder wie man sie nun bezeichnen mag nicht generalisierend beurteilen kann.

In unserer Zeit der Globalisierung ist der Protest nicht mehr an die physische Versammlung an einem Ort gebunden und damit unterliegen die Teilnehmer auch nicht der gleichen Rechtsordnung. Ebenfalls ist die Motivation der Teilnehmer womöglich sehr heterogen. Die einen nehmen aus Protest teil, um auf einen Misstand aufmerksam zu machen, auf den sie *auf dem herkömmlichen Wege* keine Änderung bewirken können - andere nehmen teil, um gezielt ihnen unsympathischen Konzernen einen wirtschaftlichen Schaden beizufügen. Insofern fällt der Vergleich mit den

"gewaltfreien" Protesten gegen den Vietnamkrieg schwer und man muss zwischen einer großen Zahl an Sonderfällen unterscheiden.

Der Geist der Gesetze

Abschließend kann man die These aufstellen, dass eine Person, wenn sie nach dem Prinzip des *Interesses am eigenen Selbst* an den Angriffen teilgenommen hat und dabei als StaatsbürgerIn eines Landes gegen das Gesetz verstoßen hat, sich dabei aber nicht - zum Beispiel durch Anonymisierung im Internet - der Strafverfolgung entzogen und auch keine Gewalt angewendet hat - im Rahmen des "zivilen Ungehorsams" gehandelt hat. Dies wäre dann nicht als Straftat zu werten.

Arendt beschreibt im dritten Abschnitt ihres Aufsatzes, wie ziviler Ungehorsam einzuordnen ist:

- "Jeder Zusammenschluß von Menschen, sei er sozialer oder politischer Art, verläßt sich letzten Endes auf die menschliche Fähigkeit, Versprechen abzugeben und Versprechen einzuhalten." (Arendt 2000: 313)

Dies ist das Prinzip, wie sich ein Staat konstituiert. Es gibt jedoch auch Situationen in der sich der Bürger seiner "einzigsten Verpflichtung [...] Versprechen einzugehen" (Arendt 2000: 313) entbinden kann. Und zwar ist das der Fall, wenn "unerwartete [Umstände] eintreten" (Arendt 2000: 313) oder wenn "die Gegenseitigkeit, die allen Versprechen zu Grunde liegt" (ibd.) beendet wird. In diesem Zusammenhang lässt sich auch der zivile Ungehorsam rechtfertigen. Arendt verweist auf den Begriff "Geist der Gesetze" (Arendt 200: 307) den Montesquieu beschrieben hat. Er entspricht einem "Konsens als Ergebnis des Gesellschaftsvertrages" (ibd.). Nach ihm gibt es eine Grundgesinnung, nach der die Gesetze verfasst wurden. In diesem Geist ist ziviler Ungehorsam zumindest in den USA zu rechtfertigen, jedoch "scheint der Versuch, [...] ihn auf rein gesetzlicher Grundlage zu rechtfertigen, auf unüberwindliche Schwierigkeiten zu stoßen" (Arendt 2000: 318). Diese Schwierigkeiten stellen eine Herausforderung an die Gesellschaft dar und werden unsere derzeitigen Staatssysteme auf den Prüfstand stellen.

Ethisch ist die *Operation Payback* schwer einzuordnen. Auch in den österreichischen Gesetzen gibt es einen zugrundeliegenden Geist, der

Dinge wie Meinungsfreiheit vorsieht. Die Operation erfüllt zwar auch einige Kriterien des zivilen Ungehorsams, doch ist er, selbst wenn dieser dem *Geist der Gesetze* entspräche, rein rechtlich betrachtet ein Gesetzesbruch. Das Umgehen mit so einer neuen Situation muss sich wohl in der Zukunft herausbilden und bewähren.

4. Synthese und Ausblick: Moderne Zeiten

Diese Form des digitalen Aktionismus ist für uns neu. Man würde gerne bestehende Konstrukte auf ihn anwenden, um gleich eine Einordnung in Kategorien wie *gut* oder *böse* treffen zu können. Der Vergleich mit einer Sitzblockade vor dem Firmeneingang scheint hierbei am nächsten zu liegen: Eine große Anzahl an Personen organisiert sich, um im öffentlichen Raum eine Funktion des öffentlichen Lebens zu blockieren. Einmal wird die Blockade durch physische Überlastung des Zugangs einer Firma hergestellt und im anderen Fall durch technische Überlastung des Firmenauftritts im virtuellen Raum. Doch genau hier ist auch der Schwachpunkt dieser Analogie: Zur Teilnahme an einer Sitzblockade muss man sich an einen bestimmten Ort begeben und ordnet sich damit auch der entsprechenden Rechtsordnung unter. Der virtuelle Raum ist jedoch global und grenzüberschreitend. Ein Geist der Gesetze ist im *Global Village* bisher nicht vorhanden, da in jedem Land mit dem Internet anders umgegangen wird.

Der Versuch, das Geschehene in Arends bestehende Theorie einzuordnen wirft neue Fragen auf. Die Möglichkeiten politischer Partizipation haben sich mit der Verbreitung des Internet als grenzenloses Netzwerk drastisch geändert. Die digitale Revolution ist ein Prozess, der uns viele neue Möglichkeiten bringt, unsere Gesellschaft zu vernetzen und

Informationen auszutauschen. Sie bringt aber für unsere Gesellschaft auch die Notwendigkeit mit sich, auf diese Veränderung zu reagieren.

Quellen

Literatur:

Arendt, Hannah (2000): *Ziviler Ungehorsam*. In: In der Gegenwart: Übungen im politischen Denken II. München [etc.]: Piper. S. 283 - 321

Martens, Ekkehard (2000): *Ich denke, also bin ich. Grundtexte der Philosophie*. München: Beck.

Internet:

FoxNews.com (2010): *FoxNews.com - Hackers Target WikiLeaks 'Enemies': Mastercard, Twitter, Paypal, Even FoxNews.com*. [<http://www.foxnews.com/scitech/2010/12/08/wikileaks-supporters-launch-hack-attacks/>] (20. Februar 2011)]

Janssen, Jan-Keno (2011): *DDoS-Attacken gegen Wikileaks-Blockierer | c't*. [<http://www.heise.de/ct/artikel/Ionenkanonen-gegen-Wikileaks-Gegner-1153351.html>] (15. Februar 2011)]

Janssen, Jan-Keno, Kuri, Jürgen & Schmidt, Jürgen (2010): *Operation Payback: Proteste per Mausklick | c't*. [<http://www.heise.de/ct/artikel/Operation-Payback-Proteste-per-Mausklick-1150151.html>] (11. Januar 2011)]

PayPal | Blog (2010): *Update on PayPal site status*. [<https://www.thepaypalblog.com/2010/12/update-on-paypal-site-status/>] (20. Februar 2011)]

postfinance.ch (2010): *PostFinance - press101206*. [<http://www.postfinance.ch/de/about/media/press/press2010/press1012061.html>] (20. Februar 2011)]

WikiLeaks, *WikiLeaks*. [<http://213.251.145.96/>] (11. Januar 2011)]

WikiLeaks, *WikiLeaks - About*. URL: [<http://213.251.145.96/About.html>] (11. Januar 2011)]

ZEIT ONLINE (2010): *Hacker-Angriffe: Ermittler zahlen es der Operation Payback heim | Digital | ZEIT ONLINE*. [<http://www.zeit.de/digital/internet/2010-12/wikileaks-hacker-festnahme-niederlande?page=all>] (16. Februar 2011)]