Das Internet als Faktor des sozialen und kulturellen Wandels - Seminararbeit bei
Prof. Dr. Hans Geser; FS 2012, Soziologisches Institut, Universität Zürich

Protestformen im Cyberspace

Möglichkeiten und Grenzen aus zivilgesellschaftlicher Sicht

Hernani Marques

Abgabedatum: 30.6.2012

Inhaltsverzeichnis

1 Einleitung

Im Jahr 2011 sollen einem Artikel im **heise online**-Magazin gemäss im **Cyberspace** *massiv* mehr Datensätze "gestohlen" [1] worden sein als noch im Jahr zuvor. Dabei wird auf den "Verizon 2012 Data Breach Investigation"-Bericht Bezug genommen, welcher Jahr für Jahr mehrere hundert Fälle von *Cyberattacken* auswertet, die von Unternehmen gemeldet werden. Der Grossteil geht im Jahre 2011 auf sogenannten *Hacktivismus* zurück, auf *politisch motiviertes Hacking*. Es wird gar vom "Jahr des Hacktivisten" gesprochen. [2;3]

Was sind *Hacktivisten*?

Hacktivisten sind *Hacker*, die politische Motive verfolgen, mitunter gesellschaftliche Umwälzung fordern. (Vgl. Martucci 2007: 53ff.)

Hat (politisches) *Hacken* nun immer die Form des Einbruchs in Computersysteme oder des Blockierens von Webseiten? Diesen Eindruck mag seit den Vorgängen des Jahres 2011, die **Anonymous** berühmt gemacht haben, manche Person haben.

Doch: Ist das so einfach?
Wenn das *nicht* so ist, welche *Protestformen* gibt es noch, von wem werden sie genutzt - und wie treten diese in Erscheinung?
Das sind die Fragen, die ich im Rahmen dieser Arbeit beantworten möchte.

Der **Cyberspace** erweitert den Raum der *Protestformen*. Insbesondere seit das Web in den 1990er Jahren im Internet Einzug hält, sind einer breiten Bevölkerungsschicht, die von der *digitalen Kluft* nicht betroffen ist (vgl. Geser 2010), einfache Möglichkeiten an die Hand gegeben ihren Unmut gegenüber den *Herrschenden* und

[1] Im eigentlichen Sinne des Wortes ist es nicht möglich Daten zu stehlen, denn sie bleiben, sofern sie nur kopiert und nicht gelöscht werden, an der Quelle vorhanden. Der Begriff hat somit moralischen (wertenden) Gehalt und muss mit Vorsicht genutzt werden.

[2] *Hacktivisten haben 2011 mehr Daten geklaut als Kriminelle*. URL: `http://www.heise.de/newsticker/meldung/Hacktivisten-haben-2011-mehr-Daten-geklaut-als-Kriminelle-1478471.html` (24.06.2012)

[3] *2011 Was the Year of the "Hacktivist", According to the "Verizon 2012 Data Breach Investigations Report"*. URL: `http://www.prnewswire.com/news-releases/2011-was-the-year-of-the-hacktivist-according-to-the-verizon-2012-data-breach-investigations-report-143761886.html` (24.06.2012)

Mächtigen zum Ausdruck zu bringen.

In den Unterkapiteln der Einleitung mache ich zuerst auf den Gegenstand der sozialen Erscheinungen, die ich betrachte, aufmerksam; in der Folge grenze ich diesen von anderen (ähnlichen) Erscheinungen ab, um den Fokus der Arbeit zu verdeutlichen.

1.1 Gegenstand

In den Medien ist tagtäglich von *DDoS-Attacken*, *SNS-Kampagnen*, *Cyberangriffen* und mitunter gar *Cyberterrorismus* die Rede.

Was hat es mit diesen Begriffen auf sich, wie effektiv sind die dahinterstehende Aktionen? Wie steht der *Cyberprotest* zu konventionellen *Protestformen*, die sich physischen *Face-to-face*-Kanälen bedienen?

Wie kaum je zuvor in der Geschichte können gar einzelne Personen, die determiniert sind, eine Botschaft an die Weltbevölkerung zu richten [4], mit vertretbarem Aufwand (in Geld und Zeit) Kampagnen lancieren, die bei entsprechender Differenzierung (gegenüber anderen bisherigen Kampagnen) oder einem Achtungserfolg erhört werden, und damit (kurzfristig) das Machtgefüge stören. (Vgl. Geser 2004: 13)

Das ist insofern ein Fortschritt, als dass in der Vergangenheit (relativ) mittellose Personen oder Gruppen zu weitaus gewalttätigeren Protestformen gegriffen haben, um auf ihre Anliegen aufmerksam zu machen - im Extremfall mit (physischen) Anschlägen.

Nicht mehr nur *ökonomisches* [5] und *soziales Kapital* [6] determinieren die *Chancen* eine medial-wirksame Kampagne zu lancieren, sondern *kulturelles Kapital* [7] ist im **Cyberspace** die treibende Kraft. [8] Wer die *sozialen* und *technischen* Mecha-

[4] Bei sehr auffälligen Aktionen werden diese Nachrichten auch in den Nicht-Online-Kanälen publik.

[5] Materielle Ressourcen wie Geld und Vermögen

[6] Die Möglichkeit über (ausgebaute) Beziehungsnetze auf materielle Ressourcen anderer zuzugreifen

[7] Immaterielle Ressourcen wie Bildung und Wissen

[8] Frei nach den Kapitalformen Pierre Bourdieus (geb. 1930)

nismen im **Cyberspace** beherrscht, kann (kurzfristig) *Macht* erlangen - wie diese genutzt wird, entscheidet letztlich über die *Legitimität* der Online-Manifestation.

Die Frage ist berechtigt: Kann durch *Cyberprotest* die *Zivilgesellschaft* gestärkt werden?

1.2 Fokus und Aufbau

Diese Arbeit legt ihren Fokus nicht auf jene *sozialen Zusammenhänge*, die den **Cyberspace** mehr unterstützend verwenden, am ehesten aber durch ihre Aktivitäten in der physischen Welt bekannt sind. So verwenden heute Parteien und Umweltschutzverbände das Internet massgeblich ebenfalls dafür sich zu organisieren und Protest zu vollziehen. Winter (2010: 101) spricht in solchen Fällen von Protestaktivitäten, die "Internet-enhanced" sind. Viele Gruppen mobilisieren ihre Aktivisten für Demonstrationen oder zum Unterschriftensammeln über den **Cyberspace** - ohne diesen als ihr natürliches Habitat zu haben.

Inhaltlich im Fokus dieser Arbeit sind Kulturen, die einen originären Ursprung in der *Hackerszene* haben und heute (zusammen) auffällig eine *transnationale Öffentlichkeit* bilden - im Speziellen seit der **Cyberspace** zunehmend von Staat und Wirtschaft beansprucht und diese eine entsprechende Reglementierung dafür fordern. (Vgl. Winter 2010: 27ff.)

Einer genaueren Analyse der Motive oder der Natur des *Hackers*, wie diese Martucci (2007: 26ff.) vorgenommen hat, stellt sich diese Arbeit nicht - der Umfang würde ungemein steigen.

Zunächst stehen im Zentrum einzig *zivilgesellschaftlich*-agierende Zusammenhänge, die dem **Cyberspace** inhärent sind und die sich organisatorisch als Vereine fester oder weniger fest in Form (dynamischer) Netzwerke organisieren. Diese haben gemeinsam, dass sie sich offen politisch äussern oder Aktivitäten verpflichtet sind, die politisch wahrgenommen werden.

Methodologisch macht sich diese Arbeit zum Ziel speziell die vielfältigen *Protestfor-*

men zu kategorisieren und am (theoretischen) Beispiel zu illustrieren; im Rahmen des empirischen Teils führe ich die Zusammenhänge der Betrachtung ein und zeige Aktivitäten auf, die sich (real) im **Cyberspace** manifestiert haben. Ich lege dabei ein besonderes Augenmerk auf die *sozialen Zusammenhänge*, die in den letzten Jahren stark polarisiert haben, wie etwa dem schwer fassbaren Kollektiv **Anonymous** und die **WikiLeaks**-Plattform um dessen Gründer Julian Assange (geb. 1971).

In Kapitel 4 erfolgt eine Diskussion anhand der empirischen Beispiele. Dabei wird im Ansatz eine Folgenabschätzung - hinsichtlich der *Chancen* und *Gefahren* - der *Protestformen* betrieben; zum einen für die betrachteten Zusammenhänge, zum anderen für die Gesellschaft als Ganzes.

Im Schlussteil (Kapitel 5) fasse ich die wichtigsten inhaltlichen Punkte noch einmal zusammen und lege meine Erkenntnisse dar. Ein Blick in die Zukunft wohnt diesem Teil ebenso inne, denn der *Cyberprotest* macht keinen Anschein ein Ende zu nehmen.

2 Theorie

> *[...] Nutzt also auch diesen Event, um mit dem Hirn Positionen zu entwickeln und klug zu argumentieren; findet den Mut im Herzen, diese Positionen gegen den Mainstream und die allgemeine Gleichgültigkeit zu vertreten und habt die Hand an der Tastatur, um die gemeinsamen Ziele auch durch Aktionen im Netz zu erreichen.*
> (Fix 2011: 12)

2.1 Gegenstand

In diesem Teil wird ein theoretisches Grundgerüst dazu geliefert, die Existenz verschiedener *Protestformen* zu begründen und zu verstehen, wieso diese in eine (logische) Rangordnung gebracht werden können.

Um ein Rahmenwerk zu konstruieren, das die Analyse von Protest im **Cyberspace** strukturiert, bedient sich diese Arbeit den Gedankengängen eines Aktivisten aus dem Umfeld des **CCC**. Die Arbeit, welche ich als Rahmenwerk verwende, um den Protest einzuteilen, ist ein Vortrag von Bernd Fix (geb. 1962), Ehrenmitglied des Chaos Computer Club Zürich [9] und *Hacker* des **CCC** in seinen Anfängen; er macht Protestformen in der realen (physischen) Welt aus und stellt Vergleiche zur (virtuellen) Welt im **Cyberspace** an. Auf der Basis wird die *Legitimität* von Protest diskutiert und Formen des Protestes, die im virtuellen Raum stattfinden, topologisiert. (Fix 2011)

Fix fordert in dem Zusammenhang den Protest nicht alleine an seiner Form dingfest zu machen und zu verurteilen, sondern grundsätzlich *Form* vom *Inhalt* zu trennen und dann zu beurteilen. Er nimmt eine zivilgesellschaftliche Sicht der Dinge (von unten) ein und verspricht sich von einer Diskussion, die auf *Inhalte* fokussiert, mehr zivilgesellschaftliches Gewicht.

Fix (2011: 6ff.) erwähnt acht - zugleich - *Eskalations-* als auch *Legitimationsstufen*, welche von einer Protestbewegung (in der Regel) in der gegebenen Reihenfolge durchlaufen werden. Jede weitergehende Stufe stellt eine Steigerung in der "Heftig-

[9] *VV_2012-05-29*. URL: `https://www.ccczh.ch/VV_2012-05-29#jungfranckianer-Antrag_bzgl._der_Ehrenmitgliedschft_f.C3.BCr_Bernd` (26.06.2012)

keit" des ausgeübten Protests dar. Diese *Eskalationsstufen* werden im Folgenden in ihrer Essenz und in einer eigenen Umschreibung sowie (in einigen Fällen mit angepassten) Begrifflichkeiten und neuen Beispielen ausgeführt.

Die (potenzielle) *Eskalation* nimmt generell mit jeder Stufe zu, wohingegen die *Legitimität* mit jeder Stufe abnimmt, oder anders ausgedrückt: Je höher das *Eskalationspotenzial* ist, desto weniger Akteure beteiligen sich am Protest in der Form. Das bedeutet, dass die *Legitimität* (und damit Akzeptanz) für konfliktivere *Protestformen* geringer ausfällt.

2.1.1 Meinungsäusserung

Bei der *Meinungsäusserung* geht es um die simple (individuelle) Äusserung der freien (politischen) Meinung, was sowohl mündlich, schriftlich als auch symbolisch erfolgen kann. Das Halten eines regimekritischen Vortrags, das Verfassen eines entsprechenden Textes mit Publikation im Internet, das Tragen von Buttons auf der Kleidung oder - im **Cyberspace** - die Platzierung von politischen Bannern auf der eigenen Webseite, können Ausdruck dieser *Protestform* sein. Dass in vielen Ländern die Möglichkeit auf die (freie) *Meinungsäusserung* gar nicht erst gegeben ist, kann bereits Anlass sein auf eine höhere Proteststufe auszuweichen.

2.1.2 Petition

Bei der Petition wird eine Aggregation konvergierender Meinungsäusserungen in einer Form betrieben, dass diese breiter erhört werden und damit die *Legitimität* höher ist, um daraus Handlungen zu fordern - z. B. eine Aufforderung gegenüber den Politikern oder der Bevölkerung ein Gesetz anzupassen.

Weit gefasst, kann damit in der Schweiz auch jede Form des Unterschriftensammelns verstanden werden, das letzten Endes zu einer Volksinitiative oder zum Zustandekommen eines fakultativen Referendums führt. Im Internet existieren Protestnetzwerke, auf die ich im empirischen Teil am Beispiel von **Avaaz.org** grob eingehe, die dafür genutzt werden können lokale Probleme global zu thematisieren. Nicht immer ist der Erfolg von Online-Petitionen (unmittelbar) gegeben, was auch damit zusammenhängt, dass diese Form des Protests eine sehr niederschwellige

Form von *Cyberprotest* überhaupt darstellt. (Vgl. Geser 2011: 10)
Praktisch jede Person kann innerhalb von Sekunden sich einer Sache solidarisch erklären, ohne sich weitere Gedanken machen zu müssen. Zudem minimiert die mangelnde *Verifizierbarkeit* der abgegeben Stimmen die *Glaubwürdigkeit* und damit die *Legitimität* einer Online-Petition ungemein.

2.1.3 Graffiti

Bei dieser Protestform wird der legale Rahmen in den meisten Ländern gebrochen. Für den **Cyberspace** spricht Fix von "Web-Graffitis" (auch: "Tags"), die an Webseiten angebracht werden können, um auf eine Sache aufmerksam zu machen. In motivationeller Hinsicht legt Martucci (2007: 40ff.) Vergleiche nahe, dass es sowohl Sprayern (aus der physischen Welt) wie auch *Hackern* (in der virtuellen Welt) um die (gegenseitige) *Anerkennung* und dem "Thrill" gehen kann, sich der Gefahr erwischt zu werden auszusetzen.

Technisch - im **Cyberspace** - betrachtet, handelt es sich bei diesen Vorgängen um *Defacements* - das ist das Entstellung einer Webpräsenz. Gelingt es einem Aktivisten eine Sicherheitslücke in den Webapplikationen einer Webseite zu finden oder in den Webserver einzudringen, so ist es diesem möglich die Präsenz - in ihrer Darstellung - einer Unternehmung (kurzfristig) zu stören. Der Vergleich zum physischen Graffiti scheint insofern gelungen, als dass die Möglichkeit gegeben ist eine - idealerweise - stark frequentierte Stelle im physischen Raum ebenso mit einer Botschaft derart zu versehen, dass diese alle Passanten sehen (müssen). Die medialen Auswirkungen sind ähnlich.

Diese Protestform hat *Zwangscharakter* und unterstreicht, dass eine erhöhte Eskalationsstufe erreicht ist. Anders aber als im physischen Raum ist ein "Web-Graffiti" in aller Regel schneller (restlos) entfernt. Dafür hat das *Dafacement* im Web den entscheidenden Vorteil bei sehr stark frequentierten Webseiten ein globales Publikum zu erreichen und somit auf ein Anliegen potenziell breit aufmerksam zu machen. Zusätzlich kommt hinzu, dass viele Webseiten dermassen unzureichend geschützt sind, dass der Aufwand eine solche Tat zu begehen, minimal sein kann und solchenfalls (in Zeit und Geld) in keinem Verhältnis dazu steht ein physisches Graffiti (klar sichtbar) an einer Stadtmauer zu hinterlassen.

2.1.4 Demonstration

Bei der *Demonstration* handelt es sich um eine *Protestform*, die dem physischen Raum inhärent zu sein scheint, wie Fix feststellt; es ist im **Cyberspace** zwar möglich an bekannten Orten, z. B. auf *Social Networking Sites* (*SNS*), zu "demonstrieren", indem verschiedene Akteure zu einer gegebenen Zeit politische Äusserungen machen, doch stellt sich dabei die Frage, ob diese Äusserungen ein valides Äquivalent zu Strassendemonstrationen darstellen, wo einer willkürlichen Öffentlichkeit eine Botschaft kundgetan wird.
Sehen wir von virtuellen Online-Welten wie **Second Life** ab, wo verschiedene *Avatare* sich aufmachen können eine Strasse entlang zu laufen und sich einer Sache zugehörig zu zeigen, scheint ein adäquates Äquivalent dieser *Protestform* für den **Cyberspace** nicht zu existieren. Das gilt insbesondere auch deshalb, weil die *Exit-Option* immerzu gegeben ist. (Vgl. Geser 2011: 10)
Wenn viele Benutzer auf **Facebook** über ihre Pinnwände "demonstrieren", indem sie im gleichen (kurzen) Zeitraum Äusserungen von sich geben, so können diese in entsprechende *Feeds* verschoben werden, die sich der **Facebook**-Nutzer nicht länger anzuschauen braucht. Das Ganze wird verschärft dadurch, dass bei *SNS*-Seiten generell jeder Benutzer seinen ganz eigenen Ausschnitt der Realität hat, bestimmt durch seinen virtuellen Freundeskreis, oder im Falle von *Microblogging*-Diensten wie **Twitter** festgelegt durch die anderen **Twitter**-User, denen er folgt.

Sollten in einer virtuellen Welt, die aus nur einem virtuellen Raum für alle besteht - etwa **Second Life** - grosse Demonstrationen vom Zaun brechen, so ist es auch da möglich sich auszuklinken. In der physischen Welt lässt sich ein Protestzug als *Demonstration* nicht einfach abschalten oder ohne Weiteres ignorieren. Im Falle massiver *Demonstrationen* werden auch weite Teile des *einzigen* physischen Raumes eingenommen, in welchem jede Person *einzig* lebt. Der *Zwangscharakter* dieser Eskalationsstufe behauptet sich nur im physischen Raum - soweit. In der Empirie zum später dargelegten *Cyberprotest* bleibt diese Stufe also ohne Beispiel und wird demnach übersprungen.

2.1.5 Streik / Boykott

Der *Streik* oder *Boykott* beschreibt Fix als eine der einfachsten *Protestformen*, denn sie zeichnet sich anstatt durch *Handeln* durch *Nicht-Handeln* aus; darüber hinaus ist diese *Protestform* vom legalen Standpunkt her betrachtet zumeist unproblematisch, sofern der juristische Tatbestand der "unterlassenen Hilfeleistung" [10] nicht vorliegt.

Der Unterschied zwischen den Begriffen *Boykott* oder *Streik* ist schliesslich keiner, der sich in der Form der *Nicht-Handlung* äussern würde. Die Unterscheidung wird nach den sozialen Räumen gemacht, in denen Akteure bewusst *nicht* handeln. Von *Boykott* wird meist im Zusammenhang mit dem (freiwilligen) Konsum von Gütern gesprochen, dann, wenn Personen sich entscheiden diese (bewusst) nicht mehr in Anspruch zu nehmen; *Streik* wird üblicherweise im (unfreiwilligen) Angestelltenverhältnis ausgeübt - er spielt im Zusammenhang mit Lohnarbeit und bei Arbeitskämpfen eine tragende Rolle; als Druckmittel, um Forderungen durchzusetzen. (Vgl. Jung 2011)

Das kann eintreten, wenn wichtige (kritische) ICT-Infrastruktur einer (kontinuierlichen) Administration Bedarf, die im Falle eines Protestes nicht länger erfolgt. Ein Extrembeispiel: In einem Spital weigert sich das ICT-Personal Online-Systeme aufrecht zu erhalten, in einem Fall, wo Bedarf nach menschlicher Intervention vorliegt. In einem solchen Fall kann das Leben von Menschen bedroht sein.

Diese *Protestform* ist aber nicht deshalb erhöhter Eskalationsstufe, weil sie durch *Nicht-Handeln* besonders kritische ICT-Infrastrukturen unnütz machen kann, sondern, weil sie ganz *generell* das Potenzial hat (profitable) Strukturen, die alleine durch die *Cyberwelt* existieren, zu ruinieren.

Um das **Facebook**-Beispiel in diesem Zusammenhang aufzugreifen: Wenn sich von heute auf morgen eine kritische Zahl Nutzer dazu entscheiden hinsichtlich **Facebook** wortwörtlich "nichts" mehr zu tun, in dieser Welt nicht mehr zu *handeln*, so bricht das gesamte Geschäftsmodell des *Web 2.0*-Riesen, das auf eine kontinuierliche Preisgabe von (möglichst privaten) Daten beruht, ein; die milliardenschwere

[10] In Deutschland StGB §323c; in der Schweiz StGB 128 "Unterlassung der Nothilfe"

Börsennotierung würde verschwinden. Derselben Herausforderungen stehen auch andere Dienste, wie **eBay** oder **Amazon**, gegenüber.

Diese Unternehmen existieren praktisch durch den **Cyberspace** und hängen *fundamental* von den Handlungen und der Interaktion ihrer Kunden ab. Genauso wie es in der physischen Welt möglich ist bewusst *nicht* zu handeln, funktioniert das im **Cyberspace** - mit ähnlichen Auswirkungen.

Diese *Protestform* hat insofern eine gegenüber anderen Akteuren aufzwingende Komponente als dass bereits eine kritische Masse "Nicht-Handelnder" ausreichen kann, um ein System zu Fall zu bringen; es ist nicht unbedingt notwendig, dass nach der Mehrheitsregel [11] ein System boykottiert wird. Im Falle der erwähnten wirtschaftlichen Unternehmen könnte ein grösserer Boykott (einer kritischen Zahl der Kundenbasis) dazu führen, dass der Dienst in der Unfähigkeit sich den neuen Bedingungen rasch anzupassen, Konkurs anmelden müsste. Damit wären die Dienstleistungen der Unternehmung für andere Personen, die sich dem *Boykott* nicht angeschlossen haben, auch nicht mehr nutzbar.

2.1.6 Sitzblockade

Die Sitzblockade hat den Charakter auf ähnliche Auswirkungen aus zu sein, wie der *Streik* oder *Boykott*, nur wird hier (nicht länger) auf die Freiwilligkeit der *Nicht-Handlung* gesetzt.

Ein Beispiel in Bezug auf die physische Welt kann sein: Ist der Aufruf einer Gruppierung gescheitert einen Supermarkt zu boykottieren, da nicht mehr einzukaufen, so kann die Gruppe auf diese Eskalationsstufe umsteigen, um den physischen Zugang zum Supermarkt mit einer kritischen Masse an Akteuren so zu stören, dass interessierte Käufer nicht mehr in den Supermarkt gelangen. Die Wirkung, die erzielt wird, kann dieselbe sein: Der Supermarkt erleidet unter dem (erzwungenen) Nicht-Verkauf wirtschaftlichen Schaden.

Ähnliches ist im **Cyberspace** praktizierbar, nur kann dort der Protest in der Regel wesentlich konzentrierter erfolgen, denn: Auch grössere Detailhändler verfügen in

[11] Wie einer repräsentativen Demokratie üblich

der Regel nur über eine Webseite (je Land), in der sie die Produkte zum Verkauf anbieten. Gelingt es einem *Netzwerk* im **Cyberspace** über ausreichend lange Zeit einen Webdienst für andere Käufer unzugänglich zu machen, so hat dies einen ähnlichen Effekt wie im physischen Raum.

Technisch handelt es sich dabei um einen Angriff der Art *Distributed Denial of Service* (*DDoS*), wo mehrere Akteure unter Einsatz ihrer Zeit (oder mittels einer Software) wiederholt Zugriffe auf den lahmzulegenden Webdienst ausführen. Dabei kommt es zu einer Überlastung des Servers, so dass die Webseite unter der Last zusammenbrechen kann.

Dass dies - verbunden mit den anderen bisher erwähnten *Protestformen* - einer Unternehmung *ökonomischen* und *symbolischen* Schaden zufügen kann, wird in der Magisterarbeit von Hillgärtner (2001) anhand des rasant fallenden Aktienwerts einer Firma im Rahmen des **Toywar** zu Weihnachten 1999/2000 ausgeführt. Zuvor kam es zu einem Rechtsstreit wegen eines Domainnamens, der letztlich mit *Cyberprotesten* - auch unter Einsatz von *DDoS*-Attacken - des Künstlerkollektivs **eToy** gegenüber dem an der Börse milliardenschwer-kapitalisierten Spielzeugdienstleister **eToys Inc.** überraschend so endete, dass die Unternehmung nachgab. Es kann vermutet werden, dass der um mehrere Milliarden Dollar reduzierte Börsenwert der Unternehmung Mitschuld daran trägt, dass **eToys Inc.** rund ein Jahr später Konkurs anmelden musste. [12]

2.1.7 Selbstermächtigung

Fix spricht hier von der “Inanspruchnahme von legitimen Rechte” und untermauert seine Ausführungen mit Beispielen aus dem Leben von Mahatma Gandhi (geb. 1948), welcher nicht erst darauf gewartet hat, dass Recht gesprochen wird, sondern sich Recht genommen hat.

Es ist ein Unterschied zu machen zwischen was *legal* ist, im Sinne des Gesetzes und was *legitim* ist, im Sinne der Moral. Es ist naheliegend, dass die moralischen

[12] *Das Spiel ist aus. Das amerikanische Internet-Spielwarengeschäft will nächste Woche Konkurs anmelden.* `http://www.manager-magazin.de/unternehmen/it/0,2828,119928,00.html` (28.06.2012)

Vorstellungen - in Anbetracht der existierenden Weltanschauungen - weit auseinanderklaffen können. Es ist auch nicht Aufgabe dieser Arbeit Aktionen in gesetzlicher oder moralischer Hinsicht zu bewerten, die sich dieser Eskalationsstufe bedienen; Tatsache ist, dass diese *Protestform* existiert und gerade in letzter Zeit im **Cyberspace** breiten Einsatz findet.

Wann immer sich ein *sozialer Zusammenhang* über die *geltende Ordnung* hinwegsetzt und stattdessen eine *legitime Ordnung* herstellt, hat das naturgemäss Konfliktpotenzial, denn es ist eine Absage gegenüber den *Herrschenden* - ein direkter Angriff auf deren *Macht*.

Eine aktuelle und regelrechte Serie von Beispielen ist mit dem Gut der *Informationsfreiheit* zu sehen - dem Recht sich aus beliebigen Quellen zu informieren. Folgt man der *Hackerethik*, wie sie der **CCC** heute führt, so geht aus Punkt 1 hervor, dass "der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, [...] unbegrenzt und vollständig sein [sollte]". [13]

Ein Beispiel der *Selbstermächtigung* auf der Grundlage dieser Ethik kann sein, dass die Dinge bei dieser Maxime nicht belassen werden, sondern, dass Gelegenheiten ausgenutzt werden, einen *Informationsgleichstand* direkt und selber herzustellen - ohne die Konsultation der *Herrschenden*. Dadurch, dass man (durch Wissen) die Macht hat, Dinge auf direktem Wege und selber zu verändern, wird es getan. *Netzwerke* wie **Anonymous** oder Plattformen wie **WikiLeaks** sind insbesondere in den Jahren 2010/1 stark mit dieser Art des Vorgehens aufgefallen. Was es mit diesen Erscheinungen genauer auf sich hat, wird aber erst im empirischen Teil dieser Arbeit erläutert. Im darauf folgenden Kapitel 4 wird dann auch eine Diskussion über die Chancen und Gefahren dieser Art des Protests geboten. Insbesondere bei **Anonymous** sind Aktionen auszumachen, die andere Regeln der Hackerethik brechen und Hackerkreise somit in ein Dilemma stürzen.

Diese Kategorie schliesst den Einbruch in Computersystemen mit der anschliessenden Publikation darauf vorgefundener (brisanter) Informationen mit ein - diese Kategorie der *Protestform* kann aber auch schlicht bedeuten, dass Informationen veröffentlicht werden, die aus anderen Quellen (seitens Informanten oder "Whistle-

[13] *hackerethics*. URL: `https://www.ccc.de/hackerethics/` (28.06.2012)

bowler") stammen. Wird in einer Unternehmung intern z. B. elektronisches Material kopiert und der Öffentlichkeit zugespielt, ist dafür kein (raffinierter) Einbruch in ein Computersystem notwendig. Die Auswirkungen für die Unternehmung sind nichtsdestotrotz ähnlicher Art.

2.1.8 "Terrorismus"

Als die "heftigste Aktionsform" (Fix: 11) können Begriffe wie "Terrorismus" hindeuten. Sowohl Fix als auch Martucci weisen darauf hin, dass dem Begriff keine klare Bedeutung zukommt (Martucci 2007: 59).

Bei dieser letzten Eskalationsstufe geht es darum wichtige Personen oder kritische Infrastrukturen einer Gesellschaft so auszuschalten, dass eine Umwälzung der herrschenden Ordnung möglich wird. In der realen Welt können dazu Akte der Gewalt gegen Personen oder Anschläge auf wichtigen Infrastrukturen wie Strom- oder Wasserversorgung eingesetzt werden. Was den **Cyberspace** betrifft, werden (vornehmlich aus militärischen Kreisen) Begriffe wie *Cyberterrorismus* angewandt, um so manche der zuvor beschriebenen *Protestformen* kollektiv zu fassen. Das erscheint unscharf und wird der Sache nicht gerecht, denn: Die meisten kritischen ICT-Systeme einer Gesellschaft sind nicht direkt an das Internet angeschlossen, so dass Szenarien wie im 2007 erschienen Hollywood-Film **Stirb langsam 4.0** [14] äusserst irreal sind.

Für den **Cyberspace** sind zwar *Protestformen* denkbar, wo von einem Server nicht nur Daten runterkopiert, sondern diese (in der Folge) auch gelöscht werden - allerdings entsteht hierbei kein physischer Schaden. Es ist zwar ein destruktiver Akt, jedoch ist damit keine (physische) Gewaltanwendung und damit eine Zerstörung der Maschinen verbunden.

Grenzfälle sind vorhanden, wenn einer Person psychischer Schaden durch elektronische Mittel zugefügt wird, indem eine Person - "terrorisiert" -, ihrer Privatsphäre beraubt oder im Internet entblösst wird. Auch ist es möglich, dass Unternehmen ein massiver wirtschaftlicher oder symbolischer Verlust erwächst, falls einem Betrieb alle Daten gelöscht werden. Die komplette und direkte Zerstörung einer Existenz

[14] *Stirb langsam 4.0*. URL: `http://www.imdb.com/title/tt0337978/` (28.06.2012)

ist damit aber nicht verbunden.

Um die ICT-Infrastruktur eines Landes in einer Art zu stören, dass es physischen Gewalt- und Zerstörungsakten gleich kommt, ist der **Cyberspace** zuletzt nicht der richtige Ort - es muss auf die physische Ebene rekurriert werden, denn aus der Ferne ist ein so umfassendes Eingreifen in gesellschaftliche Vorgänge - trotz der fundamentalen Wichtigkeit des **Cyberspace** für alle Belangen unseres Lebens - nicht real.

Ähnlich wie bei der Eskalationsstufe 4 der *Demonstration* handelt es sich bei dieser Kategorie um eine, die kein Äquivalent im **Cyberspace** hat. Sie kann im **Cyberspace** nicht nur nicht übersprungen werden, sondern wird nie erreicht. Genauso wie die Kategorie 4 scheitert sie an der im **Cyberspace** nicht vorhandenen physischen Präsenz von Personen oder Gegenständen.

2.2 Die verschiedenen Protestkulturen und deren -struktur

Die wichtige Frage ist: Woher kommt der *Cyberprotest*, der hier veranschaulicht wird und wie organisiert er sich?

Ohne im Detail auf die einzelnen *sozialen Zusammenhänge* einzugehen, die im nächsten Kapitel erst porträtiert werden, lässt sich an dieser Stelle bereits etwas über die *gemeinsame Identität*, die in Einzelfällen verbindet, aussagen.

Cyberprotest kommt in vielfältigen Formen daher und deren Aktivistenstruktur ist sehr unterschiedlich. In einer quantitativen Untersuchung von Protest im **Cyberspace** weisen die Themenverteilungen und -schwerpunkte 2010 noch wenig darauf hin, dass ein neuer Schwerpunkt mit internetspezifischen Themen emergent sein könnte. Damals bewegt sich die Kategorie “Kommunikationsfreiheit” mit unter 5% noch auf Sparflamme. (Vgl. Baringhost et al. 2010: 39ff.)

Bei der *Kommunikationsfreiheit* geht es um das Recht ungehindert kommunizieren zu können. Ein wichtiger Begriff in diesem Zusammenhang ist die *Netzneutralität* - die Idee, dass der **Cyberspace** ein von Staat, Wirtschaft und anderen Gruppen

nicht kontrollierbarer Raum sein soll. Dieser Zustand des Netzes ist überhaupt Voraussetzung für die *Informationsfreiheit*, das als sein Gegenteil die *Zensur* hat.

Es ist andererseits nicht einfach möglich eine Kampagne einer Kategorie alleine zuzuordnen, wie im Falle von **WikiLeaks** selbsterklärend sein könnte: Zwar werden die Informationen im Sinne der *Kommunikations-* oder *Informationsfreiheit* publiziert, aber es handelt sich um Informationen, die bevorzugt Staaten und private Konzerne in Bedrängnis bringen - in verschiedensten Belangen wie Menschenrechts-, Korruptions- und Fragen von Kriegsverbrechen.

Es ist auch nicht einfach, den online stattfindenden Protest den verschiedenen Protestkulturen zuzuordnen. Die Autoren stellen fest, dass zur damaligen Zeit die *Neuen Sozialen Bewegungen* massgeblich am Protest beteiligt sind, wobei nicht ersichtlich wird, ob es sich dabei um Protest *im* oder *durch* den **Cyberspace** handelt. (Vgl. Baringhost et al. 2010: 41ff.)

Die bald vorgestellten sozialen Erscheinungen und deren *Akteure* haben gemein, dass sie *im* **Cyberspace** stattfinden und über gemeinsame Werte der Offenheit verfügen. Sie sind auch alle skeptisch gegenüber Autoritäten und beobachten diese scharf. In einem gewissen Sinne lässt sich sagen, dass die Gesamtheit dieser Akteure eine *Gegenüberwachung* und *Kontrolle* von Staat und Wirtschaft betreiben, sich selber aber zwischen den Öffentlichkeiten bewegen - und somit *Zivilgesellschaft* sind.

Im Rahmen ihrer gemeinsamen Themen fordern sie “Freiheit” und “Offenheit” - sie bedienen sich der verschiedenen *Protestformen*, um sich Gehör zu verschaffen und Änderungen durchzusetzen; sie beweisen damit *Protestcharakter* und agieren im Erfolgsfall als *zivilgesellschaftliches Korrektiv*.

3 Empirie

> *[...] That's the lesson of the last few years with this new radicalization. Don't give up. Have hope. Remain skeptical. Be critical of the system that dominates us all and sooner or later – if not in this generation, then in generations to come – things will change.*
> (Tariq Ali 2012, in einem Interview mit Julian Assange und Noam Chomsky [15])

3.1 Gegenstand

Im Folgenden werden diverse *soziale Zusammenhänge* vorgestellt, die der *Hackerszene* entspringen oder nahe stehen; diese werden als Fallbeispiele für den im **Cyberspace** stattfindenden Protest herangezogen, und sollen an ausgewählten Beispielen aufzeigen, welche *Protestformen* heute zum Einsatz kommen.

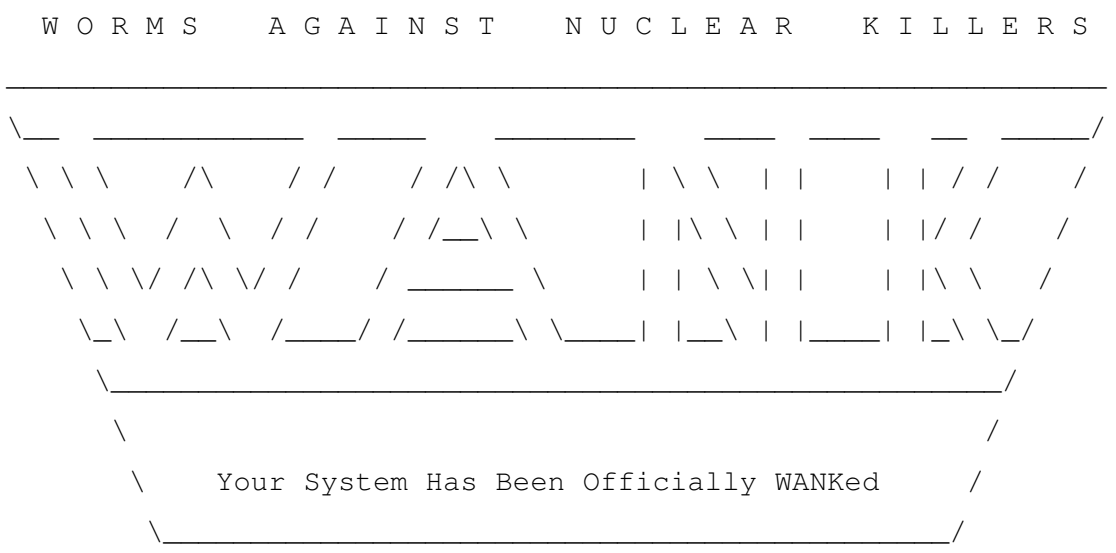
3.2 Fall WANK: Eine virulente politische Äusserung

Als einer der ersten (auffälligen) Aktionen, wo eine politische Äusserung angebracht wird, gilt der Wurm **WANK**, welcher im **DECnet** bei der **NASA** (am meisten) Verbreitung findet. Er wurde am 16. Oktober 1989 "in the wild" gesehen. [16]

[15] *Noam Chomsky tells Julian Assange: Humanity "like lemmings going over the cliff"*. URL: `http://www.rawstory.com/rs/2012/06/26/noam-chomsky-tells-julian-assange-humanity-like-lemmings-going-over-the-cliff/` (26.06.2012)

[16] *CERT Advisory CA-1989-04 WANK Worm On SPAN Network*. URL: `https://www.cert.org/advisories/CA-1989-04.html` (24.06.2012)

Beim Einloggen in ein infiziertes System wurde dem Benutzer folgendes Banner präsentiert:




```
You talk of times of peace for all, and then prepare for war.
```

Dass dessen (mutmassliche australische) Entwickler [17] (klares) politisches Bewusstsein aufweisen, wird den **NASA**-Netzwerkverantwortlichen bei der Analyse des Programms deutlich: Der Wurm ist so programmiert, dass er sich auf die "Area 48" des **DECnet** *nicht* einschleust. Dieser Teil des Netzwerks ist der neuseeländische Bereich. Neuseeland hatte sich bereits 1986 zur "nuklearfreien Zone" erklärt und machte deutlich, dass es keine Nuklearwaffen oder -technologie auf seinem Territorium dulden würde. (vgl. Dreyfus/Assange 1997: 17ff.; 27ff.)

Der Wurm hat (technische wie soziale) Ressourcen gebunden, was als *Denial of Service* (*DoS*) betrachtet werden kann. [18] Dadurch, dass der Wurm zusätzlich sich Sicherheitslücken der Systeme bedient hat, könnte man versucht sein **WANK** durchaus als erhöhte *Protestform* einzustufen, doch enthält die Aktion keine konkrete Handlungsaufforderung an die Empfänger; interessant an dem Fall allerdings ist, dass er Ansätze höherer *Protestformen* einsetzt, wie z. B. das Ausnützen von Sicherheitslücken in Systemen - weder aber wurden Daten (bewusst) gelöscht noch wurden diese kopiert und irgendwo hingeschickt.

[17] Eine bewiesene Urheberschaft ist nicht bekannt.

[18] *Intranetwork Memorandum. SPAN Management Office. Information Regarding the DECnet worm and protection measures*. URL: `http://www.textfiles.com/internet/span01.vir` (24.06.2012)

Heutzutage existiert eine aktive *Malware*-Szene mit Software, die nicht nur fähig ist beliebige Botschaften auf Rechnern zu hinterlassen, sondern auch Zugangsdaten zu beschaffen - zumeist stehen diese Aktivitäten aber im Zusammenhang mit organisierter Kriminalität im Internet oder (blindes) destruktives Wirken (oftmals seitens Jugendlicher), die ohne politische Botschaft sind.

Das Potenzial zu grösseren politischen Aktionen, die auf solche Software setzen, wäre heute noch stärker vorhanden; Fälle dieser Art, wo Protest dermassen automatisiert abläuft, fallen empirisch kaum auf. Wie die **Anonymous**-Beispiele später zeigen werden, sind Systeme zwar da die konkrete Protesthandlung zu automatisieren, nicht aber regelrecht den Protest selber. Abgesehen davon hat Protest, welcher auf Verbreitung von Würmern setzt, den Charakter wahllos zu sein - selbst wenn im Falle von **WANK** Ausnahmen eingebaut sind; in vielen (nicht bedachten) Fällen können wichtige Systeme gestört werden, welche nicht Ziel der Aktivisten sind. Das ist sicherlich mit Grund dafür, weshalb Protest seitens der hier untersuchten Zusammenhänge nicht derart verläuft.

3.3 Fall Opendata.ch: Die Initiative zu einer maschinenlesbaren Regierung

Am 19. Januar 2012 gründet sich der Verein **Opendata.ch**, welcher die kostenlose Verfügbarkeit und freie Nutzbarkeit von Behördendaten fordert und mit entsprechenden (technischen) *Hacking*-Events fördert, die ihrerseits darauf abzielen (direkt) aufzuzeigen, welches Potenzial darin liegt Behördendaten für die Bevölkerung nutzbar zu machen. Es wird in dem Zusammenhang von *direkter Datendemokratie* in der Schweiz gesprochen, der Idee also, eine Volksherrschaft über die Daten - durch direkte Datenausbeute - herzustellen. [19;20]

Weshalb erwähne ich diese Bewegung? Schon in den 1980er Jahren haben Exponenten des CCC die "maschinenlesbare Regierung" gefordert. Es blieb bei der Meinungsäusserung - mit dieser Initiative nun hat die *Open Data*-Bewegung konkrete Erfolge erzielt. Es kommt zu *Making*-Events, wo in gemeinsamen *Hacking*-Sessionen (im Sinne der Programmierung) Daten visualisiert werden und mit leicht bedienbaren (Web-)Oberflächen einer breiten Öffentlichkeit angeboten werden. Manche der Mitglieder (des Vereins) oder Aktivisten bewegen sich nun auf einer Ebene der Petition, wo sie die Herausgabe von immer mehr Daten fordern, während andere sich praktisch an die Arbeit machen aus den Daten neue Zusammenhänge zu gewinnen, die in offiziellen Statistiken (bewusst) nicht erscheinen. Auch das kann Protest sein.

Als ein konkretes Beispiel einer gelungenen Datenvisualisierung sei das Projekt "Swiss Army Contaminated Sites" erwähnt, das verschiedene Orte in der Schweiz aufzeigt, die durch das Schweizer Militär kontaminiert wurden. [21]

Nach den Grundsätzen der *Open Source*-Kultur sind die Projekte, die aus Initiativen der Bewegung entspringen, offen im Quellcode verfügbar - analog ihrer (befreiten) Behördendaten.

[19] *Vereinsgründung Opendata.ch am 19. Januar 2012 in Bern*. URL: `http://opendata.ch/2012/01/vereinsgrundung-opendata-ch-am-19-januar-2012-in-bern/` (25.06.2012)
[20] URL: `http://make.opendata.ch/` (25.06.2012)
[21] *Swiss Army Contaminated Sites*. URL: `http://make.opendata.ch/doku.php?id=project:swiss_army_contaminated_sites` (28.06.2012)

3.4 Fall Avaaz.org: Der Protest mit digitalen Petitionen

Auf dem Protestnetzwerk **Avaaz.org** [22] geben Personen Ihre Stimme [23] dafür ab an globalen Protestkampagnen teilzunehmen, um in einer konzentrierten Aktion politisch Einfluss zu nehmen. In einem Artikel hat die **Süddeutsche Zeitung** das 2007 entstandene Netzwerk um seinen Gründervater Ricken Patel porträtiert und zitiert [24] den Aktivisten (in eigener Übersetzung) wie folgt:

> *[...] Hinter fast all unseren lokalen Anliegen verbergen sich tiefere Probleme, die nur global angepackt werden können. Ein Beispiel: In Afrika bekriegen sich die Menschen um das immer knapper werdende Ackerland. Die Gründe dafür aber liegen im Klimawandel, einem globalen Phänomen. [...] Die Mehrheit der Leute ist absolut pro Umweltschutz, pro Menschenrechte und gegen Armut, Landminen und Aids. Was die nationalen Regierungen diesbezüglich entscheiden, ist leider meilenweit weg von dem, was die Menschen wollen. [...]*

Der Protest wird spürbar durch mediale Aufmerksamkeit, *einerseits* und einer *öffentlichkeitswirksamen* Übergabe der Unterschriften an die (designierten) Verantwortlichen, *andererseits* - so zumindest inszeniert es das Protestnetzwerk.

Problematisch ist, dass keine *klare* gemeinsame Linie darüber besteht, was eigentliches Fernziel von **Avaaz.org** als Ganzes ist. Oftmals sind die Themen höchst spezifisch: Einmal geht es darum eine homophobe Gesetzgebung in Uganda zu verhindern [25], ein anderes Mal - und da stellt sich **Avaaz.org** klar auf die Seite der Netzaktivisten - wird gegen **ACTA** [26] gewettert.

Bei **ACTA** handelt es sich um ein Handelsabkommen, das Produktfälschungen (durch bessere Koordination und harmonisierter Rechtsetzung) bekämpfen soll, allerdings vielen *digital natives* sauer aufstösst, da befürchtet wird, dass auf Basis dieses Vertrages gesetzliche Änderungen in den Teilnehmerländern erfolgen kön-

[22] In vielen Sprachen bedeutet dieses Wort “Stimme”.
[23] Mit Name und E-Mail-Adresse
[24] *Teil 6 von Mächtige online: “Avaaz.org - the world in action”*. URL: `http://jetzt.sueddeutsche.de/texte/anzeigen/356958` (25.06.2012)
[25] *Uganda: Rechte und nicht Unterdrückung*. URL: `https://secure.avaaz.org/de/uganda_rights/` (25.06.2012)
[26] Anti-Counterfeiting Trade Agreement

nen, das die Rechtsdurchsetzung stärker privatisiert. Die Angst ist, dass grosse (private) Rechteinhaber Informationsflüsse im Web stärker kontrollierten können und zuletzt *Zensur* erfolgt. Verantwortlich dafür ist ein Teil des Handelsabkommen, der einen verstärkten Kampf gegen Urheberrechtsverletzungen vorsieht. [27]

Frei von Kritik ist das Vorgehen von **Avaaz.org** bei solchen Kampagnen ferner nicht. Die **taz** spricht mit Bezug auf Befürwortern von **Avaaz.org**-Kampagnen von "Clicktivisten", da die Partizipationsmöglichen sehr niederschwellig sind und der Aufwand sich als Proteststimme zu manifestieren dementsprechend gering ist. [28]

Viel deutlicher als bei den bisherigen Fällen wird sich allen voran der *Protestform* der *Petition* bedient, um bei Entscheidungsträgern Änderungen zu fordern. Anders als Aktivisten anderer Zusammenschlüsse wird trotz scharfer Kritik an die Entscheidungsträger zuletzt das Gespräch mit den Autoritäten gesucht, was mit Grund dafür sein kann, dass sich sehr viele Leute den einzelnen Kampagnen anzuschliessen scheinen, die aller Länder sind - das verleiht dem Portal den Eindruck bereits heute für eine Weltöffentlichkeit zu sprechen. Effektiv finanziert sich **Avaaz.org** über Spenden und verfügt über bezahlte (freischaffende) Arbeitskräfte, die ausführend (in Vertretung aller) und organisatorisch tätig sind. Gemäss der englischen **Wikipedia** verfügt **Avaaz.org** über ein Mobilisierungspotenzial von 14 Millionen Personen - das sind die Anzahl der Kontakte, die **Avaaz.org** bisher gesammelt hat und worüber sie zu weiterem Protest (in verschiedenen) Themen aufrufen kann. [29]

[27] *ACTA: Die neue Gefahr fürs Netz*. URL: `https://secure.avaaz.org/de/eu_save_the_internet_spread/` (25.06.2012)

[28] *Avaaz.org sammelt für eigene Sicherheit*. URL: `https://www.taz.de/Clicktivisten-unter-Beschuss/!92740/` (25.06.2012)

[29] *Avaaz.org*. URL: `https://en.wikipedia.org/wiki/Avaaz` (28.06.2012)

3.5 Fall CCC / AK Vorrat: Der gesetzliche Kampf um informationelle Selbstbestimmung

Im Wiki des **AK Vorrat** zeigt eine Chronik auf, wie politische Prozesse zur zunehmenden Anwendung der *Vorratsdatenspeicherung* in Europa führen und wie sich Widerstand auf (legalem) politischem Weg dagegen (erfolgreich) formiert. Insbesondere gelingt es in Deutschland mit einer Verfassungsklage die *Vorratsdatenspeicherung* [30] vor dem Bundesverfassungsgericht für *verfassungswidrig* zu erklären. [31]

Die wichtige Rolle, welche beim Protest *Hackern* zukommt, zeigt sich zum *einen* darin, dass die **AK Vorrat** 2005 am **22C3** - dem 22. Chaos Communication Congress [32] - in Berlin gegründet wurde (auf wesentliche Initiative von **CCC**-Aktivisten) und zum *anderen* darin, dass das Bundesverfassungsgericht den **CCC** *offiziell* um ein Expertengutachten bezüglich der *Vorratsdatenspeicherung* gebeten hat. Dieses hat der **CCC** in der Folge ins Web gestellt. [33]

Der **CCC** ist der **Chaos Computer Club** und gilt seit den 1980er Jahren als eine Plattform für alle *Hacker*, die sich einem Hackerethos verpflichten. Dieser schreibt dem Schutz der Privatsphäre hohen Wert zu, was es seinen Mitgliedern verbietet sich an Aktionen zu beteiligen, welche in die Privatsphäre von Personen eingreifen. Ebenfalls verbieten sich seine Mitglieder destruktiv zu wirken und in Computersysteme so einzubrechen, dass Daten für die Öffentlichkeit (illegal) beschafft werden. Damit fügt sich der **CCC** der lokalen Gesetzgebung und hat sich als Sprachrohr und Ansprechperson für alle Belangen etabliert, wenn es um Themen des **Cyberspace** geht.

Dass der Club nicht immer so konform war, verrät ein Blick in die wechselvolle Geschichte des Clubs, insbesondere Ende der 1980er Jahre. Damals gab es

[30] Bei der *Vorratsdatenspeicherung* handelt es sich um die *verdachtsunabhängige* komplette Protokollierung von Verbindungsdaten im Bereich Telefon- oder Internetkommunikation bei den Providern - mit einer Verbindungsschnittstelle für die Behörden. Damit kann der Staat einen Überblick über das (komplette) *soziale Netzwerk* von (verdächtigen) Personen erhalten. (Vgl. Engling 2008: 67ff.)

[31] *Chronik des Überwachungsstaates*. URL: `https://wiki.vorratsdatenspeicherung.de/Chronik_des_%C3%9Cberwachungsstaates` (24.06.2012)

[32] *22C3: Private Investigations*. URL: `https://events.ccc.de/congress/2005/index.de.html` (24.06.2012)

[33] *Chaos Computer Club veröffentlicht Stellungnahme zur Vorratsdatenspeicherung*. URL: `https://www.ccc.de/de/updates/2009/vds-gutachten` (24.06.2012)

CCC-Aktivisten, die im Rahmen des **KGB-Hacks** für grosse Furore gesorgt haben. Karl Koch (geb. 1965) und einige Verbündete hatten sich zusammengeschlossen, um illegal beschaffte Daten des militärisch-industriellen Komplexes an die damalige Sowjetunion zu verkaufen. Dies hat zu viel Misstrauen geführt und der Club ist an diesen Ereignissen fast zerbrochen. (Vgl. Kulla 2003: 65ff.)

Erschwerend kommt hinzu, dass der Gründervater des **CCC** - Herwart Holland-Moritz (geb. 1951) [34] - vor diesen Ereignissen Aussagen gemacht hat, dass das im Kalten Krieg vorherrschende Informationsungleichgewicht zwischen dem Westen und dem Osten auszugleichen sei (vgl. Kulla 2003: 67ff.); es besteht die These, dass sich daraus die Handlungen der *Hacker* um Karl Koch ableiten lassen, obschon diese nicht alleine aus Idealismus, sondern auch für Geld gehackt haben.

Diese Diskussion ist bis heute nicht gänzlich abgeschlossen, wie nicht zuletzt aus dem Text von Fix (2011: 12) ersichtlich ist, wo die *Hacker* aufgefordert werden sich zusätzlichen *Protestformen* zuzuwenden und ihre Solidarität jenen Zusammenschlüssen mit ähnlicher Motivation nicht zu verweigern, die heute eskalierender vorgehen. Der Autor ist zwar zwar nicht Mitglied im **CCC** [35], er ist allerdings tief in der Geschichte des **CCC** und seinen Aktivitäten verankert.

Der **CCC** nutzt am stärksten die *Protestform* der *Petition*, ist allerdings an vielerlei Projekten beteiligt, die die *Selbstermächtigung* erlauben. Es werden nicht nur Themen der Informatiksicherheit tief und breit diskutiert - **CCC**-Aktivisten arbeiten an Software und Projekten, welche die Wahrung der Anonymität und Privatsphäre ermöglichen. So besteht zum Beispiel ein Projekt, um chinesischen Dissidenten zu helfen die *Zensur* in ihrem Land zu umgehen - das Projekt "Chinesewall". [36]
Wie das genauer funktioniert und welche (grösseren) Projekte existieren, welche die Infrastruktur dafür bieten, ist bei den Aktivisten des **Torservers.net**-Projekts, das im Folgenden vorgestellt wird, ersichtlich.

[34] Auch "Wau Holland" genannt
[35] Abgesehen seiner Ehrenmitgliedschaft beim Zürcher Ableger
[36] *CCC - China - Privacy Emergency Response Team*. URL: `http://chinesewall.ccc.de/` (28.06.2012)

3.6 Fall Torservers.net: Die technologische Selbstermächtigung zur informationellen Selbstbestimmung

Andere (rein) technisch-orientierte Aktivisten liefern die infrastrukturelle Hilfe für Cyberaktivismus aller Art: So z. B. Moritz Bartl und seine Unterstützer vom Projekt **Torservers.net**. [37] Als eine Möglichkeit die eigene Privatsphäre im Netz zu wahren, besteht nämlich unter Einsatz der **Tor**-Software, die vom **Tor-Projekt** entwickelt und quelloffen frei verfügbar ist. [38]

Ähnlich wie bei einem *VPN*-Netz ist es möglich wichtige Internetdienste nur über verschlüsselte Kanäle (oder Tunnel) zu erreichen - auf dem Weg dahin wird im Gegensatz zu einem *VPN*-Netz der Urheber im Rahmen des sogenannten *Onion-Routings* ("Zwiebel-Routing") durch verschiedene Server geleitet. Damit erfolgt nicht nur eine Verschlüsselung, sondern eine *Anonymisierung* der Verbindung. Der Betreiber des Zieldienstes kann einzig ausmachen, wie die *IP-Adresse* des letzten **Tor**-Servers [39] lautet, über die die Anfrage (effektiv, letztlich) reinkommt. Dazwischen protokollieren die **Tor**-Server i. d. R. keine Verbindungsdaten

Damit ist eine Rückverfolgung nur bis zum letzten **Tor**-Server möglich. Die einzige (realistische) Möglichkeit den Benutzer hinter den Anfragen auszumachen, ist gegeben, wenn private Informationen aus dem Inhalt der Anfrage ersichtlich werden. Das kann wiederum verhindert werden, indem für die Zieldienste verschlüssele Internet-Protokolle wie **HTTPS** (für das Surfen im Web) oder **IMAPS/POP3S** (zum Abrufen von E-Mails) verwendet werden. [40] Es handelt sich hier um nichts Geringeres als die Anti-These zur *Vorratsdatenspeicherung*, erreicht durch technische *Selbstermächtigung*.

Es kommt vor, dass das **Tor**-Netzwerk missbraucht wird, um die Identität bei Angriffen verschiedener Art zu verschleiern, doch scheint dies tatsächlich eher die

[37] URL: `https://www.torservers.net/` (25.06.2012)
[38] URL: `https://www.torproject.org/` (25.06.2012)
[39] Das ist der sogenannte *Exit-Node*.
[40] *Wie umgeht man Zensur? Moritz Bartl: "Momentan findet ein Wettrüsten statt"*. URL: `http://carta.info/37973/wie-umgeht-man-zensur-moritz-bartl-momentan-findet-ein-wettruesten-statt/` (25.06.2012)

Ausnahme darzustellen. [41]

Diese infrastrukturelle Arbeit, die also als *Protestform* im Bereich der *Selbstermächtigung* zu betrachten ist, hat ganz besonderen Wert für Aktivisten, die in ihren Heimatländern wegen ihrer politischen Meinung oder ihren Aktivitäten verfolgt werden. Die Arbeit solcher Zusammenschlüsse ist somit wichtig, um *Cyberprotest* in vielen Fällen überhaupt erst zu ermöglichen und die *informationelle Selbstbestimmung* in allen Aspekten zu wahren - aus Sicht der *Informationsfreiheit* und des (eigenen) *Datenschutzes*.

[41] *Five Years as an Exit Node Operator*. URL: `https://blog.torproject.org/blog/five-years-exit-node-operator` (28.06.2012)

3.7 Fall WikiLeaks: Informationsfreiheit durch Selbstermächtigung

WikiLeaks ist aus der Medienlandschaft nicht mehr wegzudenken. Das Portal nimmt Informationen von sogenannten *Whistlebowler* entgegen, Informanten, die auf Missstände in Staat und Wirtschaft hinweisen möchten, doch stattdessen diese gegen Geld (z. B. gegenüber Medien) zu handeln, werden diese für alle öffentlich [42] ins Netz gestellt. Die Quellen werden dabei geschützt. **WikiLeaks** betreibt dabei keinen eigentlichen Journalismus (mit Aufbereitung, weitergehender Recherche und Synthese von Informationen), sondern stellt die Informationen für alle Interessierten blank ins Netz.

Erstmals besonderes Aufsehen hat das Portal mit der Publikation des "Collateral Murder"-Videos am 5. April 2010 erregt, wo zu sehen ist, wie seitens US-amerikanischer Apache-Hubschraubern (unbewaffnete) Menschen im Irak - wie im Videospiel - getötet werden. [43].

In der Folge kam es zu weiteren spektakulären *Leaks*, wie dem "Afghan War Diary" [44] oder den "Secret US Embassy Cables" [45]. Im ersten Fall handelt es sich um Dokumente, welche die militärischen Operationen der US-Armee in Afghanistan von 2004-2010 dokumentieren. Beim zweiten *Leak* geht es um zahlreiche US-Depeschen, die von den US-Vertretungen aller Länder stammen. Viele dieser Dokumente sind eigentlich klassifiziert - heute aber im Netz frei abrufbar.

Insbesondere die USA sind über die Vorgänge erzürnt. So kursieren Informationen im Netz, dass Vorbereitungen für eine Verurteilung von Julian Assange (geb. 1971) in den USA vorliegen, obwohl seine Auslieferung in die USA nicht akut ist. [46] Julian Assange entspringt der australischen Hackerszene, die im Buch "Underground" (Dreyfus/Assange 1997) beleuchtet wird. Er hat **WikiLeaks** mit einem Hauptaugen-

[42] Gegebenenfalls anonymisiert

[43] *Collateral Murder, 5 Apr 2010*. URL: `https://wikileaks.org/wiki/Collateral_Murder,_5_Apr_2010` (27.06.2012)

[44] *Afghan War Diary, 2004-2010*. URL: `https://wikileaks.org/wiki/Afghan_War_Diary,_2004-2010` (28.06.2012)

[45] *Secret US Embassy Cables*. URL: `https://wikileaks.org/cablegate/` (28.06.2012)

[46] *New evidence of US operation against Julian Assange*. URL: `https://www.wsws.org/articles/2012/jun2012/jass-j27.shtml` (28.06.2012)

merk auf *Informationsfreiheit* aufgebaut und handelt kompromisslos. Das Motto von **WikiLeaks** auf **Twitter** lautet “We open governments.” - und das ist offensichtlich Programm. [47]

Unterstützung für das Vorgehen von **WikiLeaks** erhalten Assange und seine Mitstreiter auch von prominenter Seite. So vertrtt der bekannte Dokumentarfilmemacher Michael Moore (geb. 1954) in einem auf **YouTube** verfügbaren Video die Ansicht, dass nicht *Leaks* Menschen töten, sondern *Geheimnisse*. Als Beispiel führt er in (aus US-Sicht) gravierender Hinsicht an, dass der frühere US-Präsident George W. Bush bereits am 6. August des Jahres 2001 über Anschlagspläne, die Bin Laden hegt, informiert wurde. Daraus geht zwar nicht hervor, dass Anschläge unmittelbar drohen, aber es ist immerhin darin die Rede, dass eine Flugzeugentführung denkbar ist. Das Dokument wurde erst 2004 *entklassifiziert* und *anonymisiert* und ist in der Form heute auf **Wikisource** verfügbar; das aber erst, nach dem es schon 2002 an die Öffentlichkeit geleakt wurde. [48;49]

Einem Fernsehbeitrag von **ZDF** in der Sendung **Frontal21** geht zudem hervor, dass sowohl die spanische Zeitung **El País** als auch das bekannte (linke) Blatt **Libération** aus Frankreich den Aktivitäten von **WikiLeaks** positiv und offen gegenüberstehen. Die renommierten Blätter erachten die Vorgänge als einen wichtigen Beitrag, um *wahrheitsgetreuen* Journalismus zu betreiben und die *Pressefreiheit* zu wahren. [50] **Libération** hat sich sogar soweit mit dem Whistlebowler-Portal solidarisiert, dass sie einen Spiegelserver (“Mirror”) der **WikiLeaks**-Seite betreiben. [51]

Weiterhin ist noch schwer überschaubar, welcher Einfluss die *Leaks* auf globale Protestbewegungen und Revolutionen haben. Der Einfluss von *WikiLeaks* auf die **Jasminrevolution** z. B., die zum Sturz von Ben Ali (geb. 1936) führte, wird verschieden bewertet. In der *Blogosphäre* ist schon einmal von der “ersten WikiLeaks-

[47] URL: `https://twitter.com/wikileaks/` (28.06.2012)

[48] *Michael Moore on WikiLeaks: “Leaks Don’t Kill People, Secrets Do”*. URL: `https://www.youtube.com/watch?v=tHdPPRBDvRE` (24.06.2012)

[49] *August 6, 2001 Presidential Daily Brief. Bin Ladin Determined to Strike in US*. URL: `https://en.wikisource.org/wiki/August_6,_2001_Presidential_Daily_Brief` (24.06.2012)

[50] *Frontal21 über Anonymous - Wikileaks schlägt zurück*. URL: `https://www.youtube.com/watch?v=I5feYr8ehQA` (24.06.2012)

[51] URL: `http://wikileaks.liberation.fr/` (24.06.2012)

Revolution" die Rede. [52] Fakt ist, dass aus *Leaks* der US-Botschaft in Tunesien die (vermutete) Korruption hervorgeht. Es bleibt zu belegen, ob dies der **Jasminrevolution** zusätzlichen Aufwind gegeben hat.

WikiLeaks bedient sich ebenso der Protestform der *Selbstermächtigung*, indem es den gewünschten Zustand der Offenheit von Regierungen nicht abwartet, sondern direkt herstellt. Dass dabei ausschliesslich Dokumente veröffentlicht werden, die illegal beschafft wurden, macht das Portal für Wirtschaft und Staat zu einem wichtigen Feind.

Seit Ende 2010 kommt es zu einer grösseren Repressionskampagne gegen *WikiLeaks*. Zahlreiche Finanzdienstleister verweigern monetäre Spenden dem Projekt zuzuführen. Offenbar besteht die Idee **WikiLeaks** finanziell auszutrocknen. Dieser Vorgang bleibt allerdings nicht ohne Reaktion der Netzgemeinde - im Rahmen der **Operation Payback** und **Leakspin** kommt es seither zu Solidaritätsbekundungen bezüglich **WikiLeaks**. Diese Operationen stammen aus dem Umfeld des Kollektivs **Anonymous**, das als nächster *sozialer Zusammenhang* unserer Betrachtung die Überleitung liefert.

[52] *Tunesien: Die erste Wikileaksrevolution?* URL: `http://blog.zeit.de/leaks-blog/2011/01/14/tunesien-die-erste-wikileaksrevolution/` (25.06.2012)

3.8 Fall Anonymous / LulzSec: Informationsfreiheit durch Selbstermächtigung, digitalen Sitzblockaden und Defacements

Anonymous lässt sich am ehesten als "mitgliederlose Assoziation" charakterisieren, die geprägt ist von *Adhokratie* - einer vorübergehenden (oligarchischen) Herrschaftsform jener, die sich zusammenfinden. Die Aktivisten treffen sich in einschlägigen Foren des *Bulletin Board Systems* - speziell für das Teilen von Bilder - **4chan** im "Random"-Board /b/ [53] oder *IRC*-Chaträumen, und planen von da aus ihre Angriffe, die sie im Namen aller ausführen, unabhängig der ständigen Anwesenheit all der Assoziierten (oder Interessierten). Es geht von jenen Aktivisten der grösste Einfluss aus, denen es gelingt einen *kontinuierlichen Kommunikationsfluss* über längere Zeit (oder zum richtigen Zeitpunkt) aufrecht zu erhalten. Diese sind fähig das *Agenda-Setting* zu bestimmen und das Bild von **Anonymous** nach aussen über die Zeit ihrer gebildeten Konstellation zu prägen. (Vgl. Geser 2004: 12)

Eine detaillierte historische Aufarbeitung der Ursprünge von **Anonymous** aus **4chan** liefern die **Spiegel**-Redaktoren Reissmann/Stöcker/Lischka (2012) in ihrem Buch "We are Anonymous.". Eine detaillierte Aufarbeitung an dieser Stelle würde den Rahmen dieser Arbeit gewiss sprengen. Die Ursprünge von **Anonymous** weisen allerdings darauf hin, dass dem Spass wichtigen Rang gebührt. Teilnehmer der **4chan**-Boards, denen nachgesagt wird *Trolle* zu sein, sind für einige berüchtigte Aktionen bekannt, die als sehr invasiv gelten und jeglichem Bewusstsein für den Respekt gegenüber anderen oder den Bedürfnissen von Privatsphäre anderen trotzen. Das ist wichtig festzuhalten, um Aktionen zu verstehen, die unter dem Label **Anonymous** laufen.

Die Spiegelautoren (Reissmann et al. 2012: 7) charakterisieren **Anonymous** wie folgt:

> *[...] Manchmal verfolgt Anonymous ein übergeordnetes Ziel, eine schlichte Vorstellung von Gerechtigkeit. Immer geht es um die Freiheit des Internets, ohne Kontrolle, Schranken, Regeln. Unternehmen und Behörden, die das Netz zivilisieren wollen, fordern in den Augen der Aktivisten Angriffe heraus. Die selbsterklärten Anhänger von Anonymous betrachten es als*

[53] /*b*/. URL: `http://boards.4chan.org/b/` (28.06.2012)

> *ihre Pflicht, ihr Netz gegen Eindringlinge zu verteidigen. Doch Anonymous ist nicht nur eine Art Web-Guerilla, sondern gleichzeitig eine Subkultur, in der vor allem Spässe und Streiche, die sogenannten lulz zählen. "Lulz" kommt von "Laughing out loud" (lautes Lachen) beziehungsweise von der gängigen Internet-Abkürzung dafür: lol. Viele Aktionen haben kein übergeordnetes Ziel, Hauptsache, es gibt etwas zu lachen. Das macht Anonymous unberechenbar – und unheimlich. [...]*

Ferner ist wichtig festzuhalten, dass das Netzwerk über keinerlei (bekannten) zentralen Figuren verfügt. Es bildet Subnetzwerke heraus, die als "Operationen" bezeichnet werden und zu denen kaum Informationen vorliegen, inwiefern diese sich mit anderen Operationen oder dem Gesamtnetzwerk von **Anonymous** (personal) überschneiden.

Als sich 2008 **Anonymous** als *Protestnetzwerk* allmählich konstituiert hat, um (initial) der **Scientology-Kirche** den Kampf anzusagen, waren offenbar fünf Leute an der Ausarbeitung des entsprechenden Videos [54] beteiligt - der Zusammenhang hat sich *ad-hoc* gefunden und sowohl Form als auch Inhalt der *ersten* Botschaft bestimmt. (Vgl. Reissmann et al. 2012: 21)

Im Zuge der Operation gegen die **Scientology-Kirche** haben die Aktivisten ihr bis heute bekanntestes Symbol - die Guy Fawkes-Maske - angenommen, die heute auch bei zahlreichen Strassendemonstration immer wieder auffallen. Diese Symbolik entstammt dem Film "V for Vendetta" [55], welcher 2005 veröffentlicht wurde. In dem Film kämpft der Protagonist "Guy Fawkes" gegen ein dystopisches England der Zukunft, das totalitär regiert wird. In der Schlussszene des Films kommt es zu einem Auflauf der Massen - sie alle tragen die eine Maske. Niemand kann ausmachen, wer Guy Fawkes wirklich ist. Diese eigentlich progressive Rolle von Guy Fawkes wird unkritisch angenommen, denn seine ursprünglich historische Rolle spielt im England des 16. Jhd., wo der heutige Held eigentlich "katholischer Terrorist" war und (erfolglos) versucht hat das britische Parlament in die Luft zu sprengen. (Vgl. Reissmann et al. 2012: 7)

[54] *Anonymous Original Message to Scientology*. URL: `https://www.youtube.com/watch?v=qlJ-Yb0j3ck` (26.06.2012)
[55] *V for Vendetta*. URL: `http://www.imdb.com/title/tt0434409/` (28.06.2012)

Die zwei weiter oben angeschnittenen Operationen um **WikiLeaks** erst haben **Anonymous** einer breiten Öffentlichkeit bekannt gemacht. Zu dieser kam es, als Unternehmen angefangen haben **WikiLeaks** zu boykottieren. Eigentlich wurde die **Operation Payback** lanciert, um gegen die Unterhaltungsindustrie vorzugehen, die Mitte 2010 eine Firma angeheuert hatte gewisse Seiten mit *DDoS*-Attacken anzugreifen, welche urheberrechtich-geschütztes Material verbreiteten. Damals schreibt **The Register**, eine wichtige britische Newsseite zu technologischen Themen, dass von **4chan**-Akteuren ein Konterangriff auf Seiten der Unterhaltungsindustrie - ihrerseits mit der *Protestform* digitaler Sitzblockaden - ausgeht. [56] Der Zusammenhang hin zum Label **Anonymous** wird klar, wenn bekannt ist, dass bei **4chan** jeder Nutzer anonym - mit dem Namen "Anonymous" - Bilder posten und kommentieren kann.

Es ist allerdings nicht gültig zu behaupten, dass die Erscheinung, die heute unter dem Namen **Anonymous** als transnationale Öffentlichkeit operiert, bloss ein (politisch) ausdifferenzierter Teil des **4chan**-Netzwerks darstellt. Denn: Hinlängst kann jede und jeder Interessierte, auch ohne sich in den **4chan**-Foren zu bewegen und sich mit der dortigen Kultur auszukennen, Teil von **Anonymous** sein. In den meisten Fällen braucht man sich nur die Software **LOIC** [57] herunterzuladen, um sich als Teil des Protests einzuklinken - sofern dieser in der einfachsten Form der *digitalen Sitzblockade* ausgeführt wird. Es ist sogar möglich die Software einfach ständig laufen zu lassen, und sich einem sogenannten (freiwilligen) *Botnetz* anzuschliessen, das selbstständig Angriffe (auf beliebige) Ziele, die eine Oligarchie in Chaträumen festlegt, ausführt. (Vgl. Reissmann et al. 2012: 21)

Eigentlich ist die Software relativ simpel gestrickt und es können Gegenmassnahmen ergriffen werden. Es bleibt aber bis heute möglich unter Einsatz dieses einfachen Mittels ernstliche Blockaden zu verursachen. [58]

Die **Operation Leakspin** gilt als eine Kampagne aus dem Umfeld von **Anonymous**, die konkret darauf abzielt **WikiLeaks** zu stärken, und "[...] [s]tatt DoS-

[56] *4chan launches DDoS against entertainment industry*. URL: `http://www.theregister.co.uk/2010/09/20/4chan_ddos_mpaa_riaa/` (28.06.2012)

[57] Low Orbit Ion Cannon (dt. "Ionenkanone in niedriger Umlaufbahn")

[58] *Labs: LOIC-Attacken abwehren - DDoS im Umfeld von Wikileaks*. URL: `http://www.scip.ch/?labs.20101219` (28.06.2012)

Angriffe auf Webseiten zu verüben, [...] den Inhalt der veröffentlichten Dokumente breit [zu] streuen". So titelt **golem.de** - ein der *Hackerszene* nahestehendes Online-Magazin - sinngemäss "Info-Angriff statt DoS-Attacke". [59] In dem Zusammenhang wurden **WikiLeaks**-Dokumente aufbereitet und weitergehend gestreut - u. a. auf dem Videoportal **YouTube** oder auf *P2P*-Plattformen.

Im Zuge des Jahres 2011 kommt es dann zu der "radikalen, aggressivsten Splittergruppe" aus dem Umfeld von **Anonymous** (Reissmann 2012: 55) - zu **LulzSec**. Über 50 Tage hinweg (ebd.: 54ff.) bricht sie in staatliche und Unternehmensnetzwerke ein, kopiert (auch personenbezogene) Daten, stellt sie online und entstellt Webseiten. Es kommt auch zu *DDoS*-Attacken, die der (überschaubaren) Gruppe von rund 10 Personen zugerechnet werden. Gleichzeitig ist das ihre Schwäche, denn Ermittlungen seitens der Strafverfolgungsbehörden setzen ihr ein rasches Ende.

Im Zuge der Wirren kommt es zum sogenannten **PSN-Hack**, wo das **Playstation Network** von **Sony** angegriffen wird. Dieser Angriff wird - zumindest zum Teil - Aktivisten aus dem **Anonymous**- und **LulzSec**-Umfeld zugerechnet, sofern der Versuch einer genauen Zuordnung überhaupt sinnvoll ist. (Vgl. ebd.: 53)
Es kommt dabei zu einer massiven Veröffentlichung von Kundendatensätzen, welche ebenso Schweizer Kunden betreffen.

Denis Simonet, ehemaliger Präsident der **Piratenpartei Schweiz** (**PPS**), zitiert [60] auf seinem Blog den **Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten** (**EDÖB**) mit folgenden Worten - dies im Auszug der **EDÖB**-Antwort auf eine (öffentliche [61]) Anfrage der **PPS** hin, wie die Vorfälle um den **PSN-Hack** zu beurteilen sind:

> *Angesichts dieser aktuellen Vorfälle unterstreichen wir einmal mehr, wie wichtig es ist, dass Personendaten nur soweit bearbeitet werden dürfen, als dies für den angegebenen Zweck objektiv geeignet und tatsächlich erforderlich ist (Art. 4 Abs. 2 DSG). Diese Verpflichtung zur Datensparsamkeit*

[59] *Operation Leakspin. Info-Angriff statt DoS-Attacke.* URL: `http://www.golem.de/1012/80051.html` (28.06.2012)
[60] *Nie mehr Sony, Klappe die Vierte!* URL: `http://www.denissimonet.ch/2011/06/03/nie-mehr-sony-klappe-die-vierte/` (25.06.2012)
[61] *Sony: Offene E-Mail an den Datenschutzbeauftragten*. URL: `http://www.denissimonet.ch/2011/05/25/sony-offener-brief-an-den-datenschutzbeauftragten/` (25.06.2012)

führt dazu, dass bei Hackerangriffen oder sonstigen Datenpannen der Schaden für die Betroffen auf ein Minimum beschränkt ist.

Die **Open Security Foundation** führt eine Rangliste mit den grössten (bekanntgewordenen) Datenlecks, wo der **PSN-Hack** weit oben figuriert. [62] Dabei handelt es sich um eine *quantitative* Messung der Vorfälle - es ist im Vordergrund, wieviele Datensätze [63] blossgestellt wurden. Das misst nicht, welchen *qualitativen* Werts die Informationen sind, die preisgegeben wurden. So kann ein gezielter und weitaus unauffälliger Hack, welcher wenige, dafür brisante Informationen an die Öffentlichkeit fördert, ein höheres Schadensausmass für die involvierten Parteien bedeuten.

Wegen dem (möglichen) monetären oder symbolischen Schaden, der aus solchen Aktivitäten Wirtschaft und Staat erwachsen kann, haben sich in nahezu allen Staaten sogenannte Cyber-Abwehrzentren [64] oder -Koordinationsstellen [65] gebildet, welche die Lage beobachten und Handlungsempfehlungen abgeben. Im Falle der Schweiz besteht die **KOBIK**, welche nicht nur für den Staat und die Wirtschaft arbeitet, sondern sich auch mit dem Thema *Cyberbullying* beschäftigt, wo Individuen durch "digitales Mobbing" zu Schaden kommen. [66]

Die Aktivitäten von **Anonymous** und **LulzSec** im Jahre 2011 sind auch den Schweizer Behörden nicht entgangen. Sie werden im letztjährigen Jahresbericht zur Kriminalität in der Schweiz, im Abschnitt über "Internetkriminalität", prominent erwähnt - es wird von einer Zunahme politisch motivierter Attacken gesprochen, für die stellvertretend die beiden Zusammenhänge erwähnt werden. Nicht zuletzt ist das der Fall, weil beim **PSN-Hack** auch Schweizer Kunden zu Schaden kamen und (in Solidarität mit **WikiLeaks** und Julian Assange) Angriffe auf die **PostFinance** erfolgt sind, gleichwohl diese (exemplarischen) Vorfälle nicht (explizit) im Bericht erwähnt werden. Der beim **PSN-Hack** angerichtete Schaden schätzt das Bundesamt als "erheblich" ein. (Fedpol 2012)

[62] *Largest Incidents*. URL: `http://datalossdb.org/index/largest` (26.06.2012)

[63] Im PSN-Fall wurden etwa Name, Anschrift, E-Mail-Adresse und teils Kreditkarteninformationen öffentlich.

[64] *Nationales Cyber-Abwehrzentrum nimmt Arbeit auf* (für Deutschland). URL: `https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Cyber-Abwehrzentrum_01042011.html` (27.06.2012)

[65] *Koordinationsstelle zur Bekämpfung der Internetkriminalität* (für die Schweiz). URL: `http://www.cybercrime.admin.ch/` (27.06.2012)

[66] *Cyberbullying*. URL: `http://www.cybercrime.admin.ch/content/kobik/de/home/themen/cyberbullying.html` (27.06.2012)

Es existieren bis heute [67] **LulzSec**-Gruppen, wie etwa **LulzSec Portugal** (mit Statusmeldungen auf Twitter [68]), die nach ähnlichem Muster und vergleichbarer Motivation wie die originäre **LulzSec**-Gruppe verfahren. Sie haben bisher z. B. private Informationen über Polizisten entblösst oder Regierungsseiten mit der Platzierung politischer Botschaften entstellt. [69;70]

Im Falle von **Anonymous** und damit verbundener Zusammenhänge stellt sich zusammenfassend ein eher verwirrliches Bild. Praktisch alle nur denkbaren *Protestformen*, ausser die der *Petition*, kommen zum Einsatz. Diese *Protestform* ist für **Anonymous** mangels Ansprechpersonen nicht sinnvoll praktizierbar und passt auch nicht in das Konzept der (äusserst) aktivistischen Erscheinung, die das Netzwerk ausstrahlt.

[67] Juni 2012

[68] URL: `https://twitter.com/#!/LulzSecPortugal` (26.06.2012)

[69] *LulzSec Portugal divulga dados pessoais de 107 polícias*. URL: `http://www.tecnologia.com.pt/2011/11/lulzsec-portugal-divulga-dados-pessoais-de-107-policias/` (26.06.2012)

[70] *LulzSec Portugal volta a atacar na Madeira*. URL: `http://sol.sapo.pt/inicio/Tecnologia/Interior.aspx?content_id=52772` (26.06.2012)

3.9 Fall Estland: Die bedeutende Störung der ICT-Infrastruktur eines Landes durch digitale Sitzblockladen und Defacements?

Beim letzten hier behandelten Fall gingen die Aktivitäten von einem Netzwerk aus der Mitte einer globalisierten Gesellschaft aus, das unter keinem Label bekannt ist.

Anfangs 2007 fanden mehrwöchige *DDoS*-Attacken auf verschiedene estnische Server statt, welche wichtige Regierungs-, Banken- und *E-Government*-Seiten und -Dienste phasenweise unerreichbar machten. Zunächst sprach die estnische Regierung von einem (testweisen) *Cyberwar*, der seitens Russland gegen das kleine - stark auf neueste (Internet-)Technologien setzende Land - geführt werde. [71] Beweise dafür konnten in der Folge nie gefunden werden. [72] Effektiv zu einer (relativ milden) Geldstrafe verurteilt, wurde zuletzt ein 20-jähriger Studierender aus Estland, der als *politisches Motiv* angab mit der Verschiebung eines russischen Kriegerdenkmals nicht einverstanden zu sein. [73]

Dieser Fall ist deshalb interessant, da es im Ansatz gelungen ist ein Land alleine durch einfache elektronische Mittel kurzfristig zu destabilisieren. Die eingesetzten *Protestformen* aber zeigen, dass sie mittlerer Eskalationsstufe waren und zu keinem Zeitpunkt kritische Infrastruktur (längerfristig) lahmgelegt wurde.

Erstaunlich erscheint, dass dieser Protest offenbar nicht von Regierungsseite her erfolgt ist, sondern privat von Aktivisten gestartet wurde, die mit der Politik in Estland nicht einverstanden waren.

Dieser Fall soll insbesondere aufzeigen, dass selbst unbenannte Zusammenhänge plötzlich - wie aus dem Nichts - emergent werden können, wenn (ihnen) missliebige politische Vorgänge auffallen, sind sie noch so unwesentlich.

[71] *"In Estland wurde der Cyber-Krieg getestet"*. URL: `http://www.heise.de/newsticker/meldung/In-Estland-wurde-der-Cyber-Krieg-getestet-133482.html` (26.06.2012)

[72] *DDoS-Angriffe auf estnische Server waren kein "Cyberwar"*. URL: `http://www.heise.de/newsticker/meldung/DDoS-Angriffe-auf-estnische-Server-waren-kein-Cyberwar-138918.html` (26.06.2012)

[73] *Student für DDoS-Attacke auf Estland verurteilt*. URL: `http://www.heise.de/newsticker/meldung/Student-fuer-DDoS-Attacke-auf-Estland-verurteilt-183058.html` (26.06.2012)

4 Diskussion

> *[...] In the global commons, anonymity is an option. This is one of the great virtues of the Internet. It is also a terrible weakness. It is possible to commit crimes on the Internet anonymously. The technology that enables the Internet also undermines accountability. Given the profusion of technical knowledge, the integrity of the commons is in the hands of people whose identities we don't know, whose motives we don't understand, and whose ability to cause harm is substantial. The consequence of this will not be a glorious anarchy in the spirit of Guy Fawkes, but rather a massive repression. [...]*
>
> (George Friedman 2012, CEO Stratfor in Reaktion zum Stratfor-Hack [74])

4.1 Gegenstand

In diesem Kapitel werden einige Aspekte im Spannungsverhältnis betrachtet. Dabei werden Erkenntnisse der Funktionsweise und der Aktivitäten, wie sie die verschiedenen Zusammenschlüsse, in die in Kapitel 3 eingeführt wurde, einbezogen und ausgewogen. Der Diskussionsbedarf ist nahezu unerschöpflich. Die Arbeit beschränkt sich auf eine wichtige Auswahl und soll primär zum Nachdenken anregen.

4.2 Die Frage der Selbstermächtigung: Legitimität vs. Legalität

In seiner Dissertation stellt Meier (2011: 212) in der Betrachtung von den kürzlichen Aufständen in Ägypten die wichtige Rolle des Internets [75] bei der *Politisierung* der ägyptischen Jugend fest:

> *[...] In sum, the online youth in Egypt became a force to be reckoned with. The use of Facebook (and YouTube) helped to politicize Egyptian youth in a way that had not happened before and which mobile phones could not have done at this kind of scale. [...]*

Das obige Zitat deutet auf eine rebellische Jugend im Zuge der Proteste des **Arabischen Frühlings** hin. Viele der Proteste wurden kriminalisiert. Es gab Aus-

[74] *The Hack on Stratfor*. URL: `http://www.stratfor.com/weekly/hack-stratfor` (27.06.2012)

[75] Allen voran unter Verwendung von *Social Networking Sites* (*SNS*) wie **Facebook** oder **YouTube**

gangssperren. Was aber hat die Jugendlichen dennoch dazu bewogen weiterhin zu protestieren? Sie haben den Protest als notwendig und *legitim* empfunden.

Ähnliches begegnet uns beim Protest, der im **Cyberspace** stattfindet. Obwohl *DDoS*-Attacken in den meisten Ländern strafbar sind, obwohl das *Leaken* von (geheimen) Dokumenten nicht erlaubt ist, schliessen sich (zunehmend) Menschen zusammen und tun das, was sie für richtig empfinden.

Die *Chance* bei einem solchen Vorgehen kann darin bestehen, dass wenn der gesellschaftliche Halt genug gross ist, sich auch die gesellschaftlichen Normen (allmählich) ändern. Betrachten wir den Erfolg der *Open Data*-Bewegung in der Schweiz, so sehen Behörden zunehmend ein, dass es besser ist Datenmaterial der Öffentlichkeit zur Verfügung zu stellen, um diese einzubeziehen. Wenn die Transparenz im Staat weiter erhöht wird, sinkt das Misstrauen in die Behörden und die Grundlage für Gruppen sich Datenmaterial (illegal) zu beschaffen, wird geringer.

4.3 Die Anonymitätsfrage: Mangelnde Anerkennung vs. Gefahr der Repression

Im Allgemeinen ist es für die *Hackerkultur* wichtig von anderen Mitgliedern der Gemeinschaft erkannt und anerkannt zu werden. Das liefert Motivation für weitere Aktivitäten, im Bestreben besser zu werden und mehr zu dieser beizutragen. (Vgl. Martucci 2007: 40)

Dass es nicht unkritisch ist, sich in **WikiLeaks** involviert zu zeigen, wird im Fall von Bernd Fix deutlich: Wegen seiner Mitarbeit bei der Finanzierung des Whistlebowler-Projekts wird ihm in der Schweiz sein Job bei der für (kritische) Finanztransaktionen zuständigen Unternehmung **Six Telekurs** anfangs 2011 gekündigt. [76]

Starke Persönlichkeiten wie Bernd Fix oder Julian Assange können solchen Sanktionen widerstehen - der (positive) Medienrummel um ihre Person und ein (starker)

[76] *Der Super-Hacker*. URL: `https://www.sonntagszeitung.ch/multimedia/artikel-detailseite/?newsid=164211` (26.06.2012)

gesellschaftlicher Halt können ihnen Kraft geben, auch Rückschläge einzustecken.

Für jugendliche *Hacker*-Anwärter, die ihren Platz in der Gesellschaft noch nicht gefunden haben, kann es allerdings gefährlich sein im Zuge von *Cyberprotest* Gesicht zu zeigen, da je nach *Protestform* längere Haftstrafen drohen können, welche die Moral schwächen und Lebenswege verbauen können. Das ist insbesondere dann der Fall, wenn die Aktionen besonders destruktiver Natur waren. Bei (echten) *Hackern* ist man dann in Verruf und in der Wirtschaft kann es schwer sein eine Anstellung zu finden.

Bei Zusammenhängen wie **Anonymous** wird bewusst darauf verzichtet, sich einen grossen Namen zu machen und die Wenigen, die das versuchen, werden früher oder später gefasst, sofern sie mit (illegalen) Aktivitäten unter dem Label in Verbindung gebracht werden. Das ist insofern interessant, als dass der ansonsten bei *Hackerkulturen* übliche Geltungsdrang in dem Fall bewusst abgelehnt wird.

4.4 Die Organisationsfrage: Mangelnde Fassbarkeit vs. mangelnde Inklusion

Andreas Bogk, mitunter Sprecher vom **CCC**, macht im Rahmen eines Interviews mit der Zeitung **Die Zeit** folgende Aussage zu **Anonymous**:

> *Es ist ja keine einheitliche Organisation. Ein grosser Vorteil von Anonymous ist die Anonymität. Wenn man sich beispielsweise Projekte wie Wikileaks ansieht, erkennt man, dass diese letztlich daran zerbrochen sind, dass Leute im Rampenlicht standen und deren Ego ihnen im Weg stand. Auch der mutmassliche Wikileaks-Informant Bradley Manning wurde letztlich gefasst, weil sein Ego zu gross war und er mit seinen Informationen protzen musste. Aktionen einfach als Anonymous durchzuführen und auf den Ruhm als Privatperson zu verzichten, erhöht die Chance mit politisch brisanten Aktionen auch erfolgreich zu sein.*

Die Form der Organisation, wie sie **Anonymous** betreibt, hat den grossen Vorteil, dass es praktisch unmöglich ist das Netzwerk je zu zerschlagen, denn es sind nicht im Ansatz Führungspersönlichkeiten bekannt.

Ein Beispiel in die andere Richtung liefert **WikiLeaks**, ein zu starker "Führerkult" um Julian Assange herrscht, welcher die Organisation zur Zeit lähmt und handlungs*un*fähig macht. Auswege aus dieser Krise mag das Projekt **Friends of WikiLeaks** (**FoWL**) [77] darstellen, das sich um eine stärkere Dezentralisierung bemüht, indem eine speziell auf Privatsphäre bedachte *SNS*-Seite online geht, welche aktive Zellen von **WikiLeaks**-Unterstützern herausbilden soll. Das Projekt wurde kürzlich gestartet. [78]

Eine zu starke Dezentralisierung und zu leichtfertige *Inklusion*, insbesondere dann, wenn die Themenbandbreite zu gross ist, wie das bei **Avaaz.org** der Fall ist, hat im Gegenzug zur Folge, dass die (vielen) Aktivisten nur sehr schwach für konkrete Aktionen selber zu motivieren sind. Eine solche Struktur hängt dann von den (ausführenden) Aktivitäten jener Oligarchie ab, die das Netzwerk administrativ betreibt.

4.5 Die Frage der Wirksamkeit: Kurzfristiger vs. langfristiger Erfolg

Vorteile erhöht eskalierender *Protestformen* sind, dass grosse Aufmerksamkeit auf ein Anliegen gelenkt werden kann - das kann etwa bei den medienwirksamen *Hacks* seitens des **Anonymous**-Umfelds beobachtet werden. Es stellt sich allerdings die Frage, inwiefern diese Aktionen langfristig nützen. Diese Frage stellt sich nicht nur mit Bezug auf die Themen, die schnell ändern können, sondern auch auf die Akzeptanz der *Protestform*. Es muss damit gerechnet werden, dass die Gesetze im Bereich Internetkriminalität zunehmend verschärft werden und letzten Endes die gesamte Gesellschaft unter mehr Überwachung steht. Das schädigt dann insbesondere jene Nutzer, die weniger gut wie die *Cyberaktivisten* wissen, wie für die eigene *Anonymisierung* im **Cyberspace** zu sorgen ist.

Diese mögliche Entwicklung erscheint bisweilen grotesk, bedenkt man, dass ge-

[77] *Friends of WikiLeaks*. URL: `https://www.wlfriends.org/` (28.06.2012)

[78] *Friends of WikiLeaks: Aktivisten-Netzwerk kurz vor dem Start?* URL: `https://www.gulli.com/news/19178-friends-of-wikileaks-aktivisten-netzwerk-kurz-vor-dem-start-2012-06-28` (28.06.2012)

rade **Anonymous** mit Vehemenz versucht die Freiheit im Internet zu erhalten, die Gesetzgeber aber geradezu dazu herausfordert, ständig schärfere Gesetze zu erlassen. Selbst in der Schweiz, die von den Vorgängen weniger stark betroffen ist, liegt mittlerweile ein Postulat der Parlamentarierin Barbara Schmid-Ferer vor, die eine Reglementierung des **Cyberspace** fordert. [79]

Aktivitäten wie sie der **CCC**, als eine abgefasste und greifbare *Hacker*-Gemeinschaft, führt, verfolgen ganz ähnlichen Ziele, suchen und teilen inhaltlich viele der Anliegen, wie sie aus dem **Anonymous**-Umfeld vertreten werden, doch es wird *bewusst* darauf verzichtet destruktiv vorzugehen. Es versuchen Organisationen wie **Avaaz.org** oder der **CCC** viel stärker bzw. überhaupt die ersten Eskalationsstufen der Pyramide auszureizen und verschliessen sich dem Dialog mit den *Herrschenden* nicht. Dadurch ist ihre *Glaubwürdigkeit* höher.

Gleichzeitig bergen Organisationen, die zunehmend selber zum *Establishment* gehören, die Gefahr der zunehmenden Kompromissbereitschaft, die dazu führen kann, dass eigene Ideale - weniger wie früher - hochgehalten werden. Ein gutes Beispiel dafür ist eben der **CCC**, der verglichen mit früher - wie im Empirie-Teil von Kapitel 3 grob dargelegt - weniger radikal, dafür salonfähiger geworden ist.

[79] *Curia Vista - Geschäftsdatenbank: IKT-Grundlagengesetz*. URL: `http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113906` (28.06.2012)

5 Zusammenfassung und Schlussbetrachtungen

> *[...] They [politicians] try to get involved in issues surrounding the Internet, they call PR agencies, read the CCC's articles and try to speak the same language as the younger generation. Politicians can no longer ignore young people, which they did for a long time, and they can no longer be content to talk about networks only when raising the specter of pornography on the Internet. [...]*
> (Andy Müller-Maguhn 2011, Sprecher des CCC in einem Interview zum Club [80])

In abschliessender Betrachtung sind folgende Erkenntnisse festzustellen:
Die uns seitens Fix (2011) gelieferte Typologisierung des *Cyberprotests* erscheint fähig die wichtigsten Aktionsformen, die sich heute im Internet manifestieren, zu erfassen.

Auffällig ist, dass *soziale Zusammenhänge*, die einer personal-fassbaren Struktur sind, wie z. B. **Avaaz.org**, der **CCC**, **Opendata.ch**, **Torservers.net** oder **WikiLeaks** sich in ihrem praktizierten Protest übersichtlicher gestalten und leichter zuordnen lassen. Abgesehen eines ethischen Rahmens oder eines engen Zwecks, den sich einzelne dieser Zusammenschlüsse gegeben haben, spielt mit Sicherheit auch der Fakt eine Rolle, dass Verantwortliche benannt werden können - schliesslich bewegen sich verschiedene der *Protestformen* in einem illegalen oder doch zumindest in einem grauen Rechtsbereich. Von diesen fünf Zusammenhängen mit Abstand am meisten deviant ist die Plattform **WikiLeaks**, die sich mit der illegalen Veröffentlichung (geheimer) Dokumente mächtige Feinde gemacht hat. Alle diese Zusammenhängen weisen aber Ansprechpersonen auf - es ist möglich mit diesen in einen Dialog zu treten.

Von den verbleibenden Zusammenhängen stellen die Aktionen gegen Estland oder die Aktivisten hinter dem **WANK**-Wurm eine spezielle Kategorie dar, da in diesen Fällen praktisch nichts bekannt ist. Wie im Empirie-Teil ausgeführt, sind bei diesen Aktionen *Protestformen* im Einsatz, die stärker von der gesetzlichen Norm abweichen. Eine massiv aufwärtsgerichtete, horizontale Kommunikation mit (fast) der ganzen Palette an *Protestformen* begegnet uns mit dem (unfassbaren) Kollektiv **Anonymous** - weder sind da klare ethische Grundsätze auszumachen, noch ein

[80] *30 years of political hacking*. URL: `http://owni.eu/2011/11/08/30-years-of-political-hacking/` (28.06.2012)

bestimmter Zweck (abgesehen von Allgemeinplätzen) oder eine Führungspersonen einer irgend (feststehenden) Art. Im Rahmen von “Operationen” oder Splittergruppen kommt es zum Teil zum Einsatz heftiger Eskalationsformen, welche die Staatsmacht herausfordern. Die gewählten Organisationsformen und ihr radikales Vorgehen entbinden diese Netzwerke der Möglichkeit (oder gar Notwendigkeit) eines Dialogs.

Was nun aber den *Cyberprotest* als *Protestform* für weitergehende kulturelle oder soziale Transformation anbelangt, muss betont werden:
Eine Gesellschaft allein durch *Cyberaktivismus* im Internet umzugestalten, erscheint nach wie vor nicht real; insbesondere deshalb nicht, weil *Cyberaktivisten* naturgemäss die Möglichkeit fehlt den Mitteln (längerfristig) Herr zu werden, die den **Cyberspace** überhaupt bilden - materialisiert durch den Verbund der Rechner. Es ist zwar möglich die Kontrolle über einen Rechnerverbund zu erlangen, jedoch liegt das *Machtmonopol* zuletzt bei physischen *Akteuren* wie Polizei oder Militär. Den *Cyberaktivisten* fehlt es am nötigen *Konfliktpotenzial* für weitergehende Umwälzungen - insofern eine umfassende Umwälzung überhaupt Ziel ist.

Nichtsdestotrotz ist nicht ausgeschlossen, und die jüngste Geschichte lehrt es uns, dass Kämpfe im Netz mit solchen auf der Strasse verbunden werden können. Im Rahmen des **Arabischen Frühlings** fand nicht nur ein starker Einsatz von *Social Networking Sites* (*SNS*) statt - zur Vernetzung der eigenen Bewegung im Land, sondern es kam auch zu einer beispiellosen Solidaritätswelle von *Cyber-Protestnetzwerken*, wie **Avaaz.org**, **WikiLeaks** oder **Anonymous**, welche sich an unterschiedlichen Fronten mit eigenen *Protestformen* eingesetzt *und* den Aufständischen (mutmasslich) *informationell* und *infrastrukturell* in die Hände gespielt haben - und weiter spielen.

Es finden sich (themenspezifisch) auch immer wieder Schnittstellen der verschiedenen Zusammenhänge, die gesamthaft betrachtet als transationale Öffentlichkeit einer *Netzgemeinde* wahrgenommen werden können, die der *Hackerkultur* nahesteht und sich in Teilen (deutlich) - im Vergleich zu früheren Jahren - radikalisiert; ob zum Guten oder Schlechten für die Gesamtgesellschaft wird (noch) nicht deutlich. Das Ausmass der Aktivitäten bleibt schwer überblickbar und ist in seiner Entwicklung kaum vorauszusagen, womit es spannend im **Cyberspace** bleibt.

Literatur

[1] BARINGHOST, Sigrid / KNEIP, Veronika / NIESYTO, Johanna (2010): *Transnationale Anti-Corporate Campaigns im Netz. Untersuchungsdesign und erste Ergebnisse*. In: BARINGHORST, Sigrid / KNEIP, Veronika / MÄRZ, Annegret / NIESYTO, Johanna (Hg.): Unternehmenskritische Kampagnen. Politischer Protest im Zeichen digitaler Kommunikation. 32-62. Wiesbaden: VS.

[2] DREYFUS, Suelette / ASSANGE, Julian (1997): *Underground. Hacking, madness and obsession on the electronic frontier*. URL: `http://www.xs4all.nl/~suelette/underground/Underground.pdf` (24.06.2012)

[3] ENGLING, Dirk (2008): *Vorratsdatenspeicherung*. In: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. 67-78. Bielefeld: transcript.

[4] FEDPOL - Bundesamt für Polizei (2012): *Internetkriminalität*. In: Kriminalitätsbekämpfung Bund. Jahresbericht 2011. 29-31. URL: `http://www.fedpol.admin.ch/content/dam/data/sicherheit/jahresberichte/jabe-2011-d.pdf` (28.06.2012)

[5] FIX, Bernd (2011): *Das Internet darf kein rechtefreier Raum sein! Legitimität und Formen des politischen Protestes im Internet*. Datenspuren 2011, Dresden, 15.-16. Oktober 2011. URL: `http://aspector.com/~brf/media/2011-10-15_Datenspuren-Vortrag.pdf` (26.06.2012)

[6] GESER, Hans (2004): *Freiwillige Vereinigungen im Spannungsfeld zwischen konventionellen und neuen Medien*. In: Sociology in Switzerland. Social Movements, Pressure Groups and Political Parties. Online-Publikationen. URL: `http://socio.ch/movpar/t_hgeser4.pdf` (26.06.2012)

[7] GESER, Hans (2010): *Internet für alle - eine Illusion? Über die "digitale Kluft" und ihre Ursachen*. In: Neue Zürcher Zeitung, 247, 23 Oktober 2010, 62. URL: `https://www.zora.uzh.ch/36461/2/geser_internet_2010V.pdf` (28.06.2012)

[8] GESER, Hans (2011): *Kakaphonie und Selbstorganisation in der digitalen Agora*. In: Sociology of the Internet. Online-Publikationen. URL: `http://geser.net/intcom/t_hgeser23.pdf` (28.06.2012)

[9] HILLGÄRTNER, Harald (2001): *Netzaktivismus im Spannungsfeld von Kunst und Technik*. Magisterarbeit. 112-121. Frankfurt a. M.: Goethe-Universität.

[10] JUNG, Hans (2011): *Personalwirtschaft*. 80. München: Oldenbourg.

[11] KULLA, Daniel (2003): *Der Phrasenprüfer. Szenen aus dem Leben von Wau Holland, Mitbegründer des Chaos Computer Clubs*. Löhrbach: Werner Pieper & The Grüne Kraft.

[12] MARTUCCI, Angela (2007): *Hacking als politische Kategorie in der Informationsgesellschaft*. Liz.arbeit. Zürich: Universität Zürich.

[13] MEIER, Patrick Philippe (2011): *Do "Liberation Technologies" Change The Balance Of Power Between Repressive States And Civil Society?* Diss. Medford: Tufts University. URL: `https://irevolution.net/dissertation/` (26.06.2012)

[14] REISSMANN, Ole / STÖCKER, Christian / LISCHKA, Konrad (2012): *We are Anonymous. Die Maske des Protests - Wer sie sind, was sie antreibt, was sie wollen*. München: Goldmann. Online-Version. URL: `http://www.scribd.com/doc/82311108/dasbuchAnonymous` (26.06.2012)

[15] WINTER, Rainer (2010): *Widerstand im Netz. Zur Herausbildung einer transnationalen Öffentlichkeit durch netzbasierte Kommunikation*. Bielefeld: Winter.