

Jürgen Turek

Suelette Dreyfus/ Julien Assange: Underground. Die Geschichte der frühen Hacker-Elite.

Rezension

15. November 2011

NRW | School of Governance
www.nrwschool.de

UNIVERSITÄT
DUISBURG
ESSEN

Redaktion

Matthias Bianchi, M.A.
Tel. +49 (0) 203 / 379 - 4106
Fax +49 (0) 203 / 379 - 3179
matthias.bianchi@uni-due.de

Wissenschaftliche Koordination

Kristina Weissenbach, M.A.
Tel. +49 (0) 203 / 379 - 3742
Fax +49 (0) 203 / 379 - 3179
kristina.weissenbach@uni-due.de

Sekretariat

Anita Weber
Tel. +49 (0) 203 / 379 - 2045
Fax +49 (0) 203 / 379 - 3179
anita.weber@uni-due.de

Herausgeber (V.i.S.d.P.)

Univ.-Prof. Dr. Karl-Rudolf Korte

Redaktionsanschrift

Redaktion Regierungsforschung.de
NRW School of Governance
Institut für Politikwissenschaft
Lotharstraße 53
47057 Duisburg
Tel. +49 (0) 203 / 379 - 4106
Fax +49 (0) 203 / 379 - 3179
redaktion@regierungsforschung.de

www.nrwschool.de
www.forschungsgruppe-regieren.de
www.politik.uni-duisburg-essen.de

Rezension: Suelette Dreyfus/ Julien Assange: Underground. Die Geschichte der frühen Hacker- Elite.

Haffmans & Tolkemitt 2011, Berlin, 603 Seiten, 24,90 €, ISBN: 978-3-942989-00-8

Rezension von Jürgen Turek¹

Mit dem Einzug der Piratenpartei in das Berliner Abgeordnetenhaus 2011 rückte die Bedeutung des Internet für politische Partizipation, bürgerschaftliche Beteiligungsformen und informationelle Selbstbestimmung wieder ins Rampenlicht. Es geht den ‚Piraten‘ dabei um den Erhalt und die Pflege einer zentralen Kommunikationsplattform, die per definitionem herrschaftsfreie Aktionen und möglichst freie Umgangsformen verbürgen muss. Das Internet steht für ein Medium, das einer technologisch sozialisierten Generation ein unkontrolliertes und für das Informationszeitalter angemessenes Biotop für ihr politisches und soziales Miteinander uneingeschränkt zur Verfügung stellen soll.

Die ‚Piraten‘ (und andere) wollen nicht nur die Sicherung einer Nutzung von Social Media. Das Netz bietet vielmehr drei entscheidende Möglichkeiten politischer Partizipation und bürgerschaftlichen Engagements.

Es eröffnet *erstens* Möglichkeiten, sich Gehör zu verschaffen und ermöglicht die Offenlegung von Herrschaftspraktiken der Eliten des ‚Establishments‘, die durch ihre eigene digitale/technische Vernetzung viel verwundbarer und damit angreifbarer geworden sind. Die Herrschaft von Meinungsführern, Gatekeepern und Kommentatoren wird *zweitens* respektlos hinterfragt oder gar mit der eigenen Meinung konfrontiert. Viele ‚schnattern‘ im Netz, aber die heute politisch hochsensible Internetgeneration will es bewusst als basisdemokratisches (Macht-)Instrument zur Verfügung haben. Und als Mittel, um sich gegen politische Bevormundung oder kommerzielle Machenschaften wehren zu können, falls nötig. Hier geht es darüber hinaus *drittens* um eine bestimmte Beteiligungskultur, welche im Gegensatz zu Scheinheiligkeiten und Täuschung, Authentizität und Partizipation verlangt.² Und dies soll in Zukunft nach Meinung der Berliner und anderer Aktivisten vermutlich auch so bleiben, nicht zuletzt deshalb, weil sich viele Leute seit

¹) Jürgen Turek, M. A., ist Inhaber der TC Turek Consultant und Senior Fellow am Centrum für angewandte Politikforschung (C•A•P) der Ludwig-Maximilians-Universität München.

²) Vgl. etwa Bieber Christoph (2010): Politik digital. Online zum Bürger, Salzhemmendorf.

einigen Jahren schon etwas wohligh darin eingerichtet sowie intensiv und aus gutem Grund dafür gekämpft haben.

Web 2.0

Die weltweiten Aktions- und Protestformen mit Blick auf das WTO-Treffen in Seattle Ende der 1990er Jahre über die Widerstände gegen das G 8 Treffen (und gegen den Davos-Menschen) in Genua Anfang der 2000er Jahre bis hin zu den „Occupy-„Aktionen gegen die Wallstreet der Gegenwart haben über zwei Jahrzehnte die gewachsenen politischen Bewegungsmöglichkeiten und Einflusspotenziale der ‚Netizens‘ in diesem Sinne aufgezeigt. Große Teile von Protest und Aktion werden seit der Entwicklung des Internet selbstverständlich elektronisch organisiert. Das Netz ist vorzüglich geeignet, um international zu operieren und ansonsten unverbundene Gruppen zu koppeln. Die Freiheit der Netzwerkstrukturen garantiert Information, Beteiligung und Einflussnahme, selbst wenn mittlerweile die Kinder der Revolution - wie Google oder Facebook - selbst für Irritationen mit Blick auf Begehrlichkeiten der Verwendung von Daten sorgen. Neben der gewollten politischen Wirkungsmacht und der Unantastbarkeit der technischen Möglichkeiten sind aber auch Aspekte wie das ungestörte ‚Erwachsenwerden‘ in diesen Gruppen eine nicht zu unterschätzende Antriebskraft.

Das dürfte mit Blick auf junge politische Aktivisten zeitlos sein und hat auch der Herausbildung einer renitenten Hacker-Szene in den 1990er Jahren Schubkraft gegeben, die zunächst den PC, das Telefon und Modem und dann zunehmend das Internet direkt als Waffe einzusetzen in der Lage war. Das hatte oft nichts mit den heute üblichen Umgangsformen von Akteuren im Internet zu tun, die mittlerweile eher (fast erleichtert scheinend) im Lager der NGOs angekommen sind und ihr Enthüllungsgeschäft professionell betreiben, wie etwa WikiLeaks oder der Chaos Computerclub mit offiziellem Sitz in Hamburg.

Die Ursprünge: der Wilde Westen im Atari- und Apple-Land mit Telefon und Modem

Diesen Entwicklungspfad zeigt das Buch von Julian Paul Assange und Suelette Dreyfuss über die Entstehung des elektronischen „Underground“ in faszinierender Weise auf. Das Werk erzählt die Geschichte einer internationalen Gruppe von Hackern, die in den 1990er Jahren ihre Fähigkeiten gegen autoritäre oder als feindlich angesehene Strukturen einsetzten. Dabei sein, bei der ‚coolen‘ Avantgarde, die etablierte Herrschaftsformen herausforderte oder ihre Geheimnisse preisgab, das war eine große Antriebskraft. Dies war im Erkennen von Quellcodes und Passwörtern, im Knacken von numerischen Zugangscodes und Aufspüren von elektronischen Falltüren sowie im Zuschlagen gegen Giganten der wirtschaftlichen und politischen Welt wohl einfach unwiderstehlich. Und welche Gegner: die NASA, das Pentagon, Unternehmen wie die City Bank oder die deutsche Telekom. Das war ganz großes Kino, auch wenn es oft genug um jugendlichen Unsinn ging. Das Buch portraitiert die junge Hacker-Avantgarde, die sich in Bereiche begab, in denen vor ihnen niemand war. Ein materiell nicht fassbares und insofern ungemein reizvolles Niemandsland,

das zum Schlachtfeld wurde. Ströme von Bits und Bytes, wie es der Film Matrix später dann mit Blick auf die Ursprünge der DOS-Welt im grünlich eingefärbten Bild des vertikalen Herunterkleckerns von Zahlen und Codes irgendwie anschaulich gemacht hat. Sie waren süchtig nach dem, was sie taten, sie hackten aus politischen und persönlichen Motiven und um zu zeigen, was sie drauf hatten. So entsteht ein Kosmos von Illegalität und Besessenheit, von Triumphen und Niederlagen, von grenzenloser Neugier und Paranoia. Da entstand weltweit so etwas wie eine Familie, die auf Gedeih und Verderb fast fiebrig ihr Ding tat. Alles das vermittelt Einblicke in die Geheimnisse und das Selbstverständnis der Szene, aus denen schließlich WikiLeaks hervorging. Das waren die Desperados des Informationszeitalters, die Gesetzlosen des world wide web. Aus Australien, den U.S.A., England, Deutschland sowie Neuseeland. Auch aus Frankreich. „Par“ nannten sie sich oder „Theorem“, „Electron“, „Mendax“, „Prime Suspect“, „Pad“ und „Gandalf“ oder „Kenday oder Anthrax“. Hätten sie sich Tron genannt, wie der erste digital produzierte Hollywood-Blockbuster - es hätte nicht verwundert. Und sie kämpften durchaus um Anerkennung und Ruhm - auch gegeneinander und nicht nur mit den Autoritäten und Gegnern, die sie eigentlich auf ihren Radarschirmen ins Visier nahmen.

Die Typen, die dort wirkten, haben mit ihren Schnüffeleien zunächst für Ihre eigene Erregung und Selbstbestätigung gesorgt und ihr Imponiergehabe ordentlich versorgt. Für die Politik und die Administration waren sie im Ergebnis dann katastrophal. Zu den Urhebern dieser Unruhe gehörte Julian Assange. Doch nicht nur er allein. WikiLeaks den Boden bereitet haben eine verschworene Mannschaft von Hackern aus aller Welt, die in den 1990er Jahren mit spektakulären Aktionen das Establishment herausforderten. Und diese Aktionen waren durchaus atemberaubend, auch weil die Hacker das Klischee von unaufgeräumten und mit vollgestopften Pizzaschachteln und Bier- und Coladosen bestückten Hinterzimmern wahrscheinlich auch noch bedient haben. Sie zeigten auf, wie staatliche oder wirtschaftliche Organisationsstrukturen auf einmal wie aus dem Nichts attackiert werden konnten: durch den Angriff einer im Dunklen operierenden Macht, die Lebensadern elektronisch bombardierte, indem sie schlicht und einfach Sicherungen im System ausschalteten oder Kontrollen umgingen.

1989, etwa, plante die NASA eine wichtige Mission mit Blick auf die Erkundung des Jupitersystems und setzten dabei auf Nuklearenergie als Antriebskraft des US-Satelliten Galileo. Die frühen Aktivisten des noch nicht offiziell bestehenden Netzwerkes griffen die NASA-Operation deshalb mit dem legendären Wurm „WANK“ (Worms Against Nuclear Killers) an, um das Unbehagen der Umweltaktivisten an dieser Mission zu demonstrieren und die Durchführungsprogramme zu stören. Ein wenig Plutonium würde sich schon in der Weite des Weltalls bei einem möglichen Unfall verflüchtigen, so sagte die NASA; Jahrhunderte hoch strahlendes Material, das in das All geschossen würde, könnte genauso schnell wieder böse auf die Erde zurück fallen, meinten die Kritiker. Dem schlossen sich die Hacker entschieden an, und so störten sie massiv die Operation. Das Buch beschreibt in jeder Einzelheit, wie das in der frühen Atari-, oder Apple-Welt ging, welch heillose Verwirrung durch den Einsatz der in Hinterzimmern und Studierstuben blechern

quakenden Telefonmodems bei der NASA entstand und wie das Tauziehen zwischen Machern und Hackern auf ziemlicher Augenhöhe verlief.

Später dann, als WikiLeaks entstanden war, haben sie Spitzenpolitiker im militärischen, politischen oder im industriellen Bereich buchstäblich vorgeführt. Der Wutausbruch von US-Außenministerin Hillary Clinton nach der Veröffentlichung diplomatischen Materials durch WikiLeaks hinsichtlich der Einschätzung von Freunden wie Feinden des internationalen Parketts 2011 und die beschämten Reaktionen der bloß gestellten Regierungen sind bekannt. Dieses traditionell um äußerste Diskretion bemühte Geschäft hatte es hier auf einmal mit ‚widerlichen‘ Machenschaften zu tun. Respektlose Freaks griffen mit einer unglaublichen Chuzpe ehrwürdige Institutionen wie ein Außenministerium als Hacker oder Phreaker an und schafften unerwartet peinliche Transparenz. Der „Wilde Westen“ der Computerpiraterie der damaligen Pionierzeiten schuf dafür den Ausgangspunkt.

Andere Bubenstücke der damaligen Hackereliten rundeten das Bild einer neu auf den Plan tretenden Macht ab; die Anarchisten des Informationszeitalters, die ersten Piraten auf den Weltmeeren der Digitalisierung, waren auf den Plan getreten. Und hätten sie gewusst, wie viel Unschuld die Hackerszene noch verlieren sollte, wie viele Polizeirazzien, parlamentarische Untersuchungen, Ermittlungsverfahren und Gerichtsprozesse folgen würden, sie hätten ihre technischen Systeme wohl still abgeschaltet und diskret im damals langsam anschwellenden Fluss des Elektronikschrotts versenkt.

Dies aber taten sie in ihrem Rausch nicht. Der Zirkus wanderte weiter und verdichtete sich immer mehr zu einer unglaublichen Bedrohung des sich immer weiter vernetzenden Systems. Es verwundert deshalb nicht, das es zu einer Art Krieg zwischen Hackern und den Sachwaltern der neu entstehenden Kommunikationsstrukturen des Industriezeitalters kam, die derartige Störungen einfach nicht ertragen, geschweige denn zulassen konnten. Die ‚Admins‘ der betroffenen Stellen wurden aktiv, das FBI und die NSA traten auf den Plan. Der Kampf tobte jahrelang und ebte schließlich durch Abnutzungserscheinungen der Kombattanten und aufgrund der Möglichkeiten des Zugriffs auf die Szene ab. Diese löste sich teilweise im Chaos der damaligen Zeit auf, ihre Protagonisten mussten sich den gesundheitlichen, psychologischen und juristischen Folgen Ihrer Taten stellen. Einige machten in jeder Hinsicht Entzug, andere wanderten ab, wieder andere traten bei WikiLeaks oder woanders an. Und eine neue Generation trat auf den Plan. Ein neues Zeitalter der Netizens brach an, die sich weiterhin weder durch staatliche Stellen kontrollieren noch durch Wirtschaftsunternehmen in ihrem Konsumverhalten manipulieren lassen wollen.

„Underground“ als Antriebsmotor von Sunshine Journalism und WikiLeaks

Suellette Dreyfuss stellt am Ende des mitreißend geschriebenen und ungemein interessanten Buches fest, dass die Anfänge der Hackerwelt gemessen an heutigen Realitäten und Möglichkeiten der organisierten Kriminalität und der polizeilich/geheimdienstlichen Reaktionen darauf geradezu unschuldig und naiv wirkt. Dem kann man nur zustimmen wenn man bedenkt, dass der jährliche Schaden in diesem Bereich weltweit heute bei etwa 388 Milliarden € liegt. Neben der virtuellen Kriegsführung zur Spionage oder Sabotage ziviler und militärischer Ziele und der Wirtschaftskriminalität geraten dabei auch Privatpersonen immer öfter ins Visier von Hackern und Kriminellen aus dem Cyberspace.³ Demgegenüber aber seien die Ursprünge von Wikileaks keineswegs kriminell motiviert gewesen, auch wenn die Hacker bewusst illegales Handeln in Kauf genommen haben, sondern der erste Banträger des „Sunshine Journalism“, der helles Licht auf die Lügen und Verfehlungen von Regierungen und Unternehmen geworfen habe, indem er Originaldokumente und Fakten veröffentlichte, welche eine ungeschminkte Wahrheit zeigten.

Dahinter stehe ein Ethos, nämlich, dass Informationen frei zugänglich und allen zugänglich sein sollten. Das war und ist die Idee von WikiLeaks, das als wirkungsmächtiges Netzwerk des investigativen Journalismus schließlich zu einer großen Herausforderung für alle politischen Akteure der Wissensgesellschaft geworden ist. Suellette Dreyfuss schließt auf Seite 565 mit dem Satz: „Irgendwann in dem Jahrzehnt zwischen 2000 und 2010 wurde 1984 von George Orwell in Teilen zur Realität“. Sie bezieht sich auf Videoüberwachung, die Möglichkeit der umfassenden Überwachung des Verkehrs im Internet und per Telefon oder das Aufkommen elektronischer Scanner. All das sind schwierige Fragen moderner Governance im 21. Jahrhundert, die weitere Spannungen provozieren. Das Buch ist deshalb als Gründungsdokument einer neuen Zeit spannend und eine Quelle dafür, wie die Karriere des Internet als politisches Reizthema zwischen Regierenden und Regierten begann – und offenbar auch weitergeht.

³) Vgl. Schönbohm, Arne (2011): Deutschlands Sicherheit. Cybercrime und Cyberwar. www.mv-buchhandel.de