Civil War in Cyberspace

Ziviler Ungehorsam, innere Unruhen und Bürgerkrieg in der Informationsgesellschaft[1, 2]

Hartmut Pohl[3]

Inhaltsverzeichnis

Abstract

In der Informationsgesellschaft nehmen auch in Deutschland aggressive und kriminelle Handlungen (Computermissbrauch) ausweislich der jährlichen Kriminalstatistik [BMI02] zu. Weniger Bedeutung wird in Deutschland bisher politisch–motivierten Aktionen beigemessen.

Weltweit werden klassische Verfahren wie ziviler Ungehorsam, innere Unruhen und Bürgerkrieg zunehmend durch IT–gestützte Verfahren ergänzt und ersetzt (Transformation). Durch die weltweite Verfügbarkeit der IT–gestützten Verfahren und des Internet muss der – auf einen Staat begrenzte – Begriff des zivilen Ungehorsams genauso wie der der inneren Unruhen und der des klassischen Bürgerkriegs transformiert werden in den ubiquitären Cyberspace.

Angesichts zunehmender gewalttätiger Aktivitäten unterhalb der Kriegsschwelle im Cyberspace muss die Sensibilität für die Auswirkungen dieser Aktivitäten dringend geschaffen werden und angemessene Reaktionen müssen auf allen Ebenen (Private, Unternehmen und Behörden) erarbeitet werden.

[1] Der Verfasser dankt Herrn Prof. emer. Dr. Dr. Herbert Fiedler sehr herzlich für die Anregung zur Bearbeitung des Themas.

[2] Erschienen in: Schubert, S. et al. (Hrsg.): Informatik bewegt. Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik (GI) – Workshop 'Der Staat im Cyberspace' (Herbert Fiedler, Sayeed Klewitz-Hommelsen) S. 469 – 475. Bonn 2002

[3] Hartmut.Pohl@fh–brs.de.

1 Risiken und Aktivitäten im Cyberspace[4]

Die Informationsgesellschaft hängt ab von der Verlässlichkeit und Beherrschbarkeit vernetzter Informationstechnik von Privaten, Unternehmen oder Behörden. Infrastrukturen (die Gesamtheit zusammengehörender Einrichtungen) stellen in einem organisatorischen oder geographischen Bereich an unterschiedlichen Standorten gleichartige Dienstleistungen bereit; eine Infrastruktur wird als kritisch bezeichnet, wenn durch Einschränkung oder Ausfall Dienstleistungen nicht mehr verfügbar sind, auf die Private, Unternehmen oder Behörden aber weitgehend angewiesen sind5 [Ce97b, Ce01, Pr97].

Bedingt durch die Verletzlichkeit der Informationsgesellschaft [Ro89] können durch IT–gestützte Verfahren – insbesondere in kritischen Infrastrukturen – zusätzliche, umfangreichere und höhere Schäden[6] [W01] erwartet werden bis hin zur Auflösung jeglicher gesellschaftlicher Ordnung.

Politisch motivierte Aktivisten nutzen das Internet zur Organisation von Aktionen und Vereinigungen (network centric warfare) [AGS02] und streben darüber hinaus das Ziel der Medienüberlegenheit (information superiority) an oder zumindest besserer Informationsversorgung Interessierter [AR01]; daneben steht die Nutzung der Informationstechnik (IT) als Angriffswerkzeug gegen IT–Systeme (Information Warfare[7]) von Privaten, Unternehmen und Behörden [PC98].

Während bei klassischen Aktivitäten meist größere Menschenmengen in oder zwischen Staaten aktiv werden, können im Cyberspace dieselben oder stärkere Wirkungen von Einzelnen erreicht werden; im Cyberspace ist es unerheblich, wer und wie viele aktiv sind und welchem Staat sie angehören; staatliche Grenzen haben keine Bedeutung mehr.

Der Civil War im Cyberspace stellt einen Teilaspekt des Information Warfare dar [P98a, P00a, P00b, PC98]. Der Business Information Warfare [P00a] als Aktivität zwischen Unternehmen ist ein weiterer – hier nicht behandelter – Teilaspekt des Information Warfare. Zu einer Gesamtdarstellung des Information Warfare vgl. [P02].

Gewalt–Niveau	**Klassische Aktivitäten**	**Cyberspace**
0	Ziviler Ungehorsam, Demonstration, Sitzstreik.	Civil Disobedience, Sit–In: Mail–Verteiler, Informationsverteilung durch Web–Server, mail–flooding. Überlastung und Lahmlegen von Servern.
1	Zusammenrottung, Besetzung, Stürmen von Geländen und Gebäuden.	Hacktivism: Automatisierte e–mail Bomben, Web–Hacks (Übernahme von Webservern), unberechtigte Veröffentlichungen, Viren, Würmer.
2	Blockade: Straßen, Autobahn, Schiene, Flugplatz. Unternehmen und Behörden.	Blockading: Server, Intranet, Extranet. (Distributed) Denial of Service.
3	Innere Unruhen, Tumult. Aufruhr, Rebellion, Aufstand. Terrorismus.	Terrorism: Stören wichtiger Informationstechnik durch Lesen (und Verteilen), Ändern (bis hin zum Löschen) von Daten.
4	Guerilla. Befreiungskampf. Bürgerkrieg.	Civil War: Manipulation von Daten und Programmen der für **Teile des Staates** lebenswichtigen IT.
5	Krieg.	Information Warfare: Manipulation von Daten und Programmen der für den **gesamten Staat** überlebenswichtigen IT.

Tab. 1: Vergleich klassischer Aktivitäten mit IT–gestützten Aktivitäten im Cyberspace[8].

---

[4] Datenraum. Begriff für die Menge aller vernetzten Server und Clients mit den verarbeiteten (und gespeicherten) Daten und den Netzen (Satelliten–, Mobil–, Funk– und Festnetze – sowie Intra– und Extranets) zusammen mit den steuernden Systemen. Als Repräsentant des Cyberspace kann das Internet bezeichnet werden. Der Begriff geht auf einen Roman [Gi84] zurück.

[5] Als kritische Infrastrukturen werden z.B. diese gesehen: Energie– und Wasserversorgung, Informations– und Kommunikationswesen, Finanzbereich, Transportwesen/Logistik, Notfallversorgung/Rettungswesen, Gesundheitswesen, öffentliche Verwaltung und Regierung.

[6] Als worst case können Angriffe auf die (vergleichsweise dezentralisiert organisierte) Lebensmittel– und Wasserversorgung oder sogar die (europaweit stark vernetzte) Energieversorgung (Strom, Öl, Gas) angenommen werden.

[7] Zur Unterscheidung von klassischen Aktivitäten werden hier zur Kennzeichnung der IT–gestützten Aktivitäten im Cyberspace anglo–amerikanische Begriffe benutzt.

[8] Das jeweils höhere Gewaltniveau enthält Maßnahmen, Ziele und gewalttätige Aktivitäten der niederigeren Stufen.

Die generellen informationstechnischen und organisatorischen Risiken im Cyberspace wurden vielfach behandelt [Br98, Ce97a, Fi02]. Auf die konkreten Risiken eines Civil War geht allerdings weder der US–amerikanische Bericht zu kritischen Infrastrukturen [Pr97] noch der unautorisiert veröffentlichte Bericht der Bundesregierung [NN99] ein[9]. In diesen Untersuchungen wird ausschließlich der worst case eines totalen (Informations–)Kriegs [PC98] gegen einen Staat behandelt. Gewalttätige Aktivitäten unterhalb der Schwelle kriegerischer Auseinandersetzungen nach der Genfer Konvention (Bürgerkriege) nehmen zu und werden vermehrt erwartet [Pe95].

Die Ubiquität und Pervasivität der Informationstechnik kann schlagwortartig durch das Internet dargestellt werden, das weltweit mit geringen Kosten nutzbar ist und Zugriff auf wertvolle Daten von Privaten, Unternehmen und Behörden sowie die Steuerung des Internet selbst ermöglicht. Die informationstechnischen Risiken gründen in der Abhängigkeit von wenigen Produkten, die mit bekannten sicherheitsrelevanten Schwachstellen entworfen, implementiert, installiert und genutzt werden; Beispiele sind in den Bereichen Protokolle, Betriebssysteme, Datenbanksysteme und Anwendungssoftware zu finden.

[9] Dies gilt gleichermaßen für den Bericht des Auswärtigen Amts [An02], der auch verkennt, daß IT-Systeme als – in der Genfer Konvention von 1932 nicht anerkannte – Waffen benutzt werden können. Die Innentäterproblematik wird genauso verharmlost wie die Bildung krimineller Vereinigungen. Tatsächlich ist deutschen Behörden das Gegenteil bereits seit Mitte der 80er Jahre bekannt [PH89]. Das vom Bundesamt für IT–Sicherheit (BSI) aus dem Geschäftsbereich des Bundesministers des Innern herausgegebene e-Government Handbuch [BSI02] geht auf innerstaatliche Risiken nicht ein.

2 Transformation klassischer Handlungsweisen in den Cyberspace

Im Cyberspace ändern sich drei Aspekte.

1. Aus den klassischen Aktivitäten von Bürgerinitiativen und Non Governmental Organisations (NGO) wie dem lokal begrenzten zivilen Ungehorsam und Sitzstreiks, über innerhalb eines Staates stattfindende Zusammenrottungen, Besetzungen, Stürmen von Geländen und Gebäuden, innere Unruhen und Tumulte bis hin zu Rebellion, Aufstand und Aufruhr sowie Bürgerkrieg entwickeln sich zunehmend IT–gestützte Aktivitäten – vgl. Tab. 1.
2. Die Zielobjekte wandeln sich von physischen zu primär virtuellen – nämlich den auf Clients, Servern, Gateways, Routern und in Intranets und Extranets sowie in den Steuerungskomponenten des Internet verarbeiteten (übertragenen und gespeicherten) Daten.
3. Im Cyberspace fehlt die haptische Erfahrung sowohl des Gemeinschaftsgefühls der Aktivisten als auch der Auswirkungen des eigenen Handelns.

3 Hacktivism: Techniken und Verfahren des Civil War

Der Begriff Hacktivism [De99] kennzeichnet politisch motivierte Hacker, die Ziele allein oder in Gruppen unter Einsatz der Informationstechnik (vgl. Tab. 1) verfolgen.

So werden auf allgemein zugänglichen Servern Angriffstools angeboten, mit deren Hilfe ein Zielserver so manipuliert wird, dass er nur noch Fehlermeldungen generiert. Oder ein Angriffstool generiert viele Kommunikationsvorgänge mit einem Zielserver, überlastet ihn mit Anfragen und verlangsamt dadurch die Ladezeit, bis der Zielserver wegen dieser Überlastung nicht mehr antworten kann.

Eine funktionale Beschreibung eines der Angriffstools (FloodNet) findet sich in [St]; diese Seite ermöglicht auch die Nutzung des Produkts für Unerfahrene [Di01].

Die im Cyberspace meist nur unzureichend mögliche Identifizierung und Zuordnung der Angreifer zu einem Land erschwert eine deutliche Unterscheidung zwischen Civil War (zwischen Volksgruppen eines Staates) und Information Warfare (zwischen Staaten) – vgl. hierzu die unten erwähnten exemplarischen Fälle.

Die Angriffswerkzeuge dürften zukünftig weiterentwickelt werden – auch als Gegenangriffe [NN98]. Eine erkennbare Entwicklung stellen die stärkere Programmsteuerung (Automatisierung), das gezieltere Vorgehen und sehr schnelle Angriffe (Schwachstellenerkennung, Angriffsverteilung) dar, die binnen weniger Minuten mehr als 80% aller Server im Internet lahm legen können [SPW02] sowie das Unterlaufen von Sicherheitsmaßnahmen und Angriffe auf der Netzwerkschicht [CERT02].

4 Exemplarische Fälle

Zum ersten Mal wurde 1993 elektronischer ziviler Ungehorsam von der US-amerikanischen KünstlerInnengruppe Critical Art Ensemble untersucht [CAE94, CAE96]. Das erste dokumentierte virtuelle Sit-In veranstaltete 1995 das italienische strano.net[10], um gegen französische Atomtests auf dem Pazifikatoll Mururoa zu protestieren [M02]; der Erfolg war nur deswegen mäßig, weil das Internet noch kein Massenmedium war.

4.1 Ejercito Zapatista de Liberacion Nacional (EZLN)

Am 1. Januar 1994 besetzten Mitglieder der EZLN (auch: Intercontinental Zapatista National Liberation Army) sechs Städte in der mexikanischen Provinz Chiapas und forderten politische, ökonomische und soziale Reformen ('wahre Demokratie', 'Landreform'). Wegen fehlender klassischer militärischer Machtmittel suchte die EZLN die Informationsdominanz im 'information space'. Dazu wurden Informationen zur Situation in Mexiko im Internet verteilt [Ra00].

Zur Unterstützung dieses Bürgerkriegs organisierte u.a. die Bewegung 'Electronic Disturbance Theater' (EDT)[11] bis 1998 mehrere verteilte Angriffe (flooding) gegen die Webseite des mexikanischen Präsidenten Zedillo sowie des Präsidenten Clinton, des Pentagon und der Frankfurter Börse [EDT02]. Das Department of Defense (DoD) der USA leitete daraufhin Gegenangriffe ein [NN98]. Die bisher jüngste Aktion der EDT gegen die mexikanische Regierung fand am 31. Mai 2002 von 9.00 bis 12.00 EST statt; weitere Proteste wurden vorläufig eingestellt.

---

[10] http://www. netstrike.it

[11] U.a. unterstützt von dem Berkman Center For Internet & Society an der Harvard Law School.

4.2 eToy gegen eToys

Das 1996 gegründete virtuelle Kaufhaus für Kinderspielzeug eToys beanspruchte 1997 neben der Internet Domain eToys.com auch die von einer schweizerischen Künstlergruppe seit 1994 benutzte Adresse eToy.com, weil täglich 20.000 Kunden diese Webseite (versehentlich) anklickten. Als die Künstlergruppe dieses Ansinnen trotz eines Angebots von 530.000 US $ ablehnte, verklagte das Kaufhaus die Künstlergruppe erfolgreich. Nach einer weltweiten Pressekampagne und im Internet verbreiteten Berichten wurde das Kaufhaus im Dezember 1999 und Januar 2000 von sog. Netzaktivisten und daraufhin gebildeten Sympathisantengruppen mit sehr vielen mails überschüttet und die Server überlastet und schließlich blockiert mit dem Ziel, Bestellungen zu verhindern. Der Börsenkurs fiel am 25. Januar 2000 von in der Spitze 67 US $ auf 13 US $ [ET00, Gr00]. Abschließend zog eToys seine Klagen zurück, zahlte die Anwaltskosten der Künstlergruppe – und ging im Jahr 2002 in Konkurs[12]. Der Börsenwertverlust betrug über 20 Mrd. US $ [NN00a].

4.3 Einige andere Fälle

Portugiesische Aktivisten blockierten 1991 nach einem Massaker indonesischer Truppen auf Timor an 250 Timoresen mehrfach Server der indonesischen Behörden [NN01b].

Im Kosovo-Konflikt erpresste 1998/99 eine serbische Gruppe einen in der Schweiz angesiedelten Provider des politischen Gegners, seine Server abzuschalten [Bla00, Rö98].

Gegen die Freihandelspolitik der World Trade Organisation (WTO) protestierten 1999 auf Initiative der fünfköpfigen englischen Aktivistengruppe 'electrohippies' nach eigenen Aussagen etwa 500.000 Benutzer mit Denial of Service Attacken die Webseite der WTO [M02].

Mit dem Ziel der Anerkennung von Links auf Webseiten als Literaturverzeichnisse wurde 2000 eine 'virtuelle Sitzblockade' des Justizministeriums unter dem Motto 'Geben Sie Linkfreiheit, Frau Herta' durchgeführt[13] [Pi00, NN01a].

Chinesische Hacker gingen in 2001 mit Server–Blockaden anlässlich der Notlandung eines amerikanischen Flugzeugs gegen die US–Regierung vor wegen fortwährender Spionageflüge über chinesischem Hoheitsgebiet [Pl01].

Die EDT ist mit vergleichbaren Angriffen und Aufrufen u.a. 2002 gegen die NATO im Kosovo–Konflikt, gegen Israel im Palästina–Konflikt und am 15. Juni 2001 gegen die Lufthansa wegen des Transports (Abschiebung) abgelehnter Asylsuchender [Gr00, G01] vorgegangen. An diesen Aktionen waren nach Aussage der EDT nachweislich zwischen 15.000 und 37.000 Aktivisten beteiligt zuzüglich nicht gezählter Sympathisanten.

An israelisch–palästinensischen Aktivitäten in 2001 und 2002 wird erkennbar, dass der Unterschied zwischen Hacktivism, Terrorismus, Bürgerkrieg, Befreiungskampf und Krieg in der Praxis nicht einfach zu erkennen ist [Ge00, NN00b, Pa01].

5 Ausblick

5.1 Zukünftige Entwicklung

Neuere Angriffsverfahren lassen eine verstärkte Programmsteuerung erkennen sowie eine höhere Angriffsgeschwindigkeit durch vorangehende Schwachstellenerkennung und einer wirkungsvollen Angriffsverteilung. Weiterhin nehmen Angriffe auf der Netzwerkschicht zu.

5.2 Rechtliche Bewertung

Der Entwurf einer EU–Richtlinie [CEC02] fordert die Bestrafung von Hackern in Abhängigkeit vom angerichteten Schaden nicht unter 1 Jahr Gefängnis ohne weitere Differenzierung. Dagegen kann es sinnvoll sein, dem klassischen Demonstrationsrecht entsprechende Regelungen für den Cyberspace zu schaffen [Ca02].

5.3 Aufgaben

Es sollte untersucht werden, inwieweit zukünftig zu erwartende Angriffe (civil disobedience, hacktivism, blockading) unterhalb der Kriegsschwelle bleiben und eine Anpassung oder Erweiterung des Demonstrationsrechts auf den Cyberspace sinnvoll ist.

---

[12] Inwieweit sich hier andere Ursachen auswirkten, ist nicht bekannt.

[13] Vom Bundesjustizministerium wurde das Recht auf Online–Domonstrationen verneint [K01, NN01a].

6 Literatur

[AGS02] Alberts, D.S.; Garstka, J.J.; Stein, F.P.: Network Centric Warfare. Developing and Leveraging Information Superiority. Washington 2002

[AR01] Arquilla, J.; Ronfeldt, D.: Networks and Netwars. The Future of Terror, Crime, and Militancy. Santa Monica 2001

[An02] Antes, M.: Sicherheitspolitische Herausforderungen moderner Informationstechnologie. Berlin 2002 http://www.auswaertiges-amt.de/www/de/infoservice/download/pdf/friedenspolitik/cyberwar.pdf.

[Bla00] Blattner-Zimmermann, M.: Die sicherheitspolitische Dimension neuer Informationstechnologien. In: Holznagel, B.; Hanßmann, A.; Sonntag, M. (Hrsg.): IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen. Arbeitsberichte zum Informations–, Telekommunikations– und Medienrecht, Bd. 7. Münster 2001

[Br98] Brunner, E.: Bericht der eidg. Studienkommission für strategische Fragen. Bern 1998

[BSI02] Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.): E-Government-Handbuch. Bonn 2002. http://www.bsi.de/fachthem/egov/3.htm

[BMI02] Bundesministerium des Innern (Hrsg.): Polizeiliche Kriminalstatistik 2001. Wiesbaden 2002 http://www.bka.de

[Ca02] Cappato, Marco (Draftsman): Draft Oppinion for the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs on the proposal for a Council Framework Decision on attacks against information systems. (COM(2002) 173 C5-0271/2002 2002/0086(CNS))

[Ce97a] Cerny, D.: Information Warfare. Eine neue Bedrohung für Staat und Wirtschaft? In: Tagungsband 5. Deutscher IT-Sicherheitskongress des BSI. Ingelheim 1997

[Ce97b] Cerny, D.: Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung. Kolloquiumsvortrag 'Elektronische Informationsnetze und Infrastruktursicherheit der Bundesrepublik Deutschland'. Stiftung Wissenschaft und Politik, München 3. Dezember 1997.

[Ce01] Cerny, D.: Überlegungen zu einer Konzeption zum Schutz kritischer Infrastrukturen. In: Holznagel, B.; Hanßmann, A.; Sonntag, M. (Hrsg.): IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen. Arbeitsberichte zum Informations–, Telekommunikations– und Medienrecht, Bd. 7. Münster 2001

[CEC02] Proposal for a Council Framework Decision on attacks against information systems. Brussels, 19.04.2002 COM(2002) 173 final 2002/0086 (CNS)

[CERT02] CERT Coordination Center (Ed.): Overview of Attack Trends. Pittsburgh 2002 http://www.cert.org/nav/whatsnew.html

[CAE94] Critical Art Ensemble: The Electronic Disturbance. 1994

[CEA96] Critical Art Ensemble: Electronic Civil Disobedience and Other Unpopular Ideas. 1996

[De99] Denning, D. E.: Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Washington 1999 http://www.terrorism.com/documents/denning-infoterrorism.html

[Di01] Dion, D.: Script Kiddies and Packet Monkeys – The New Generation of 'Hackers'. Pittsburgh 2001 http://rr.sans.org/hackers/monkeys.php

[EDT02] Electronic Disturbance Theater. http://www.nyu.edu/projects/wray
Deutsche Seite: http://www.geocities.com/demo4alles/dt/index.html

[ET00] Künstlergruppe etoy.com (Hrsg.): Der Toywar – was bisher geschah. O.O. und J. http://www.simsy.ch/toywar.htm

[Fi02] Fiedler, H.: Cyber – libertär? Nach dem 11. September. Informatik Spektrum 25, 3, 215 – 219, 2002

[Ge00] Gentile, C. J.: Hacker War Rages in Holy Land. Wired Links 2000 http://www.wired.com/news/print/0,1294,40030,00.html

[Gi84] Gibson, W.: Neuromancer. New York 1984

[Gr00] Grether, R.: Wie die Etoy–Kampagne geführt wurde. 9. Februar 2000 http://www.heise.de/tp/deutsch/inhalt/te/5768/1.html

[Gr01] Grether, R.: Deportation Class. Berlin 15. Juni 2001 http://www.deportation-alliance.com/lh/grether .html

[M02] Morell, A. Online-Aktivismus: Vom virtuellen Sit-In bis zur digitalen Sabotage. O.O. und J. http://www.copyriot.com/unefarce/no5/oaktivismus.html

[NN98] N.N.: Pentagon Beats Back Internet Attack. Wired News, September 10, 1998

[NN99] N.N.: Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Arbeitsgruppe KRITIS. Entwurfsversion 7.95. Bonn 1999 (unautorisierter Bericht des BSI). http://www.koehntopp.de/kris/kritis/

[NN00a] N.N.: Der Krieg der Künstler. Wie etoy es eToys heimzahlte - eine Nachlese. Neue Zürcher Zeitung, 25. Februar 2000 http://www.nzz.ch/netzstoff/2000/netz110.html

[NN00b] N.N.: Mideast 'hacktivist' take conflict online. CNN.com Nov. 3, 2000 http://www.cnn.com/2000/TECH/computing/11/03/israel.hacking.ap/index.html

[NN01a] N.N.: Kein Demonstrationsrecht im Cyberspace? heise.de 18. Juni 2001 http://www.geocities.com/rouwer/dt/news/news.html

[NN01b] N.N.: Hackerangriffe. Hacker gegen Indonesien, USA und Rassisten. O.O. und J. http://www.ee.shuttle.de/ee/pmgymherz/Projekte/compkrim/krim/hack.html

[Pa01] Paul, L.: When Cyber Hacktivism Meets Cyberterrorism. Pittsburgh http://rr.sans.org/hackers/terrorism.php

[Pe95] Peters, R.: The Culture of Future Confict. Parameters Winter 1995 – 96, 18 – 27

[Pi00] Pifan, T.: "Virtuelle Sitzblockade" vor dem Bundesjustizministerium. Spiegel online 28. Juni 2000 http://www.spiegel.de/netzwelt/politik/0,1518,82964,00.html

[Pl01] Pluta, W.: Rache für Wang Wie. Spiegel online 30. April 2001 http://www.spiegel.de/netzwelt/politik/0,1518,131137,00.html

[P98a] Pohl, H.: Information Warfare – Information Survivability. Datenschutz und Datensicherung 2, 114 – 115, 1998.

[P00a] Pohl, H.: Business Information Warfare. In Geiger, G. (Hrsg.): Sicherheit der Informationsgesellschaft. Gefährdung und Schutz informationsabhängiger Infrastrukturen. Baden Baden 2000

[P00b] Pohl, H.: Information Warfare. In: Reinermann, H. (Hrsg.): Regieren und Verwalten im Informationszeitalter. Heidelberg 2000

[P02] Pohl, H.: Information Warfare. Stand und Zukunft. To be published 2002

[PC98] Pohl, H.; Cerny, D.: Information Warfare: Der Krieg im Frieden. In: Bauknecht, K.; Büllesbach, A.; Pohl, H.; Teufel, S. (Hrsg.): Sicherheit in Informationssystemen SIS '98. Zürich 1998

[PH89] Pohl, H.; Hütte, L.: Computer-Spionage: Ist die Katastrophe unvermeidbar? Journal für Wirtschaft und Gesellschaft – bonntendenz 4, III / 1989 http://www.inf.fh–rhein–sieg.de/person/professoren/Pohl/publicity.htm

[Pr97] President's Commission on Critical Infrastructure Protection (Ed.): Critical Foundations. Protecting America's Infrastructures. Washington 1997 http://www.ciao.gov/resource/pccip/pccip_documents.htm

[Ra00] Ramasastry, A.: Hacktivism, Virtual Protest and Organizing on the Web. IPEF Conference 'Internet and Power'. Cambridge University 2000. www.ipef.org/events/ipef2000/presentations/ ipef2000-AnitaRamasastry.ppt

[Rö98] Rötzer, F.: Von der Inszenierung des Infowar. heise online 3. 11. 98 http://www.heise.de/tp/deutsch/special/info/6305/1.html

[Ro89] Roßnagel, A.; Wedde, P.; Hammer, V.; Pordesch, U.: Die Verletztlichkeit der 'Informationsgesellschaft'. Opladen 1989

[St] Stalbaum, B.: The Zapatista Tactical FloodNet. A collaborative, activist and conceptual art work of the net. O.O. und J. http://www.thing.net/~rdom/ecd/ZapTact.html

[SPW02] Staniford, S.; Paxson, V.; Weaver, N. : How to Own the Internet in Your Spare Time. Proc. 11th USENIX Security Symp. http://www.cs.berkeley.edu/~nweaver/cdc.web.

[W01] Weber, J.: Welches Maß an IT-Sicherheit brauchen wir? Maßstäbe für die Kritikalität. In: Holznagel, B.; Hanßmann, A.; Sonntag, M. (Hrsg.): IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen. Arbeitsberichte zum Informations–, Telekommunikations– und Medienrecht, Bd. 7. Münster 2001