Kunstfreiheit statt Hackerparagraph

Miriam Ommeln und Lexi Pimenidis

Abstrakt. Wie viel Ethik steckt tatsächlich im Hacken? Sind die populären Vorurteile gegenüber Hackern berechtigt? Wir wollen zeigen, was genau beim Hacken vor sich geht und wie aus dem Hacken soziale Verantwortung entsteht, – die sowohl das ‚Conscience of a Hacker' erklärt als auch auf das Wohl der Gesamtgesellschaft gerichtet ist. Für die Rechtsprechung oder zukünftige Ethikkodizes, die nachhaltig wirken sollen, ist diese Diskussion unumgänglich.
Das Ergebnis unserer Untersuchung zeigt, dass sowohl die Thematik des Hacken, als auch die der IT-Sicherheit auf *ästhetischen* Wurzeln beruht, – nicht auf ethischen. Diese werden im Wesentlich erst später aufgesetzt. Wenn aber die Kunst mit dem Hacken verwandt ist, *sollten Hacker die gleichen Freiheiten erhalten wie Künstler*. Eine Art "Künstler-Status" scheint uns angemessener als der eines "Kriminellen".

1. Vorworte

Mit der plakativen Forderung nach Kunstfreiheit für das Forschungsgebiet der IT-Security und die Hacker soll, um einem möglichen Vorurteil zuvorzukommen, kein Blankoscheck für kriminelle Handlungen ausgestellt werden, sondern eine dringend notwendige Diskussion über das eigentliche Wesen des Hackens angestoßen werden, um juristische Korrekturen zu ermöglichen, die das digitale immaterielle Zeitalter bedingt. Technologische Entwicklungen und die Entstehung von neuartigen Werken ziehen das wiederholte Scheitern von Definitionen von *Kunst* oder *Wissenschaft* nach sich, ebenso die von *Recht*.
Die Entwicklung des Urhebergesetzes zeigt trotz seiner kurzen Historie (seit ca. Anfang des 19. Jahrhunderts) diese Problematik des neuartig Hinzukommenden – ähnlich der andauernden, unabgeschlossenen Geschichte des Kunstbegriffs, oder des Technikbegriffs. Da Definitionen in der Regel zu kurz greifen, operiert man mit einem *offenen* Kunstbegriff. Konkret bedeutet das, dass Kunst das ist, was man als Kunst bezeichnet. Pragmatisch gefasst: Kunst ist das, was im Rahmen der Institutionen und des Wirtschaftsmarktes als Kunst ausgehandelt wird. Die inhärierte Relevanz der Ökonomie innerhalb der Rechtssprechung ist ein nicht zu unterschätzendes Moment. Weil Kunst Deutung ist, ist sie damit aber auch Gericht und Urteil. Gesetze werden nicht zum Selbstzweck generiert, sondern unterliegen dem kulturellen Kontext, d.h. dem Zeitgeist. Im Übrigen ist damit auch der Begriff „kriminell" kein fixer, unabänderlicher Begriff.
Dennoch kann der Kunstbegriff nicht der Beliebigkeit anheim fallen, sondern er schließt in sich selbst das Verständnis von *Anti*kunst mit ein. Bei der Kunst des Hackens verhält es ebenso. Nicht jeder Hack erfüllt die Kriterien eines ‚echten' Hacks. Wir beziehen uns im Wesentlichen auf die Methode des Hackens, wie sie in der IT-Sicherheits-Industrie praktiziert wird.
Wir wollen im Folgenden nicht auf juristische Fragen, wie die der Schöpfungshöhe, des Werkbereichs etc. eingehen, – dieses tun wir in einer gesonderten Abhandlung und zwar indirekt; genauso wie in der Folgenden, in der wir uns auf den denkerischen Hintergrund beschränken. Diese scheinbare Beschränkung erscheint uns jedoch der Schlüssel zum Erfassen des eigentlichen Wesens des Hackertums. Wir verlassen nun den Kunstbegriff und knüpfen vorerst an den üblichen ethischen Debatten um die Hacker an.

2. Einleitung

„Die Welt will betrogen werden“ und der „*jeder Mensch ist ein Lügner*“, so lauten seit alters umgangsprachliche Sprichwörter.[1] Und die Hacker scheinen sich diese zu ihrem Motto erkoren zu haben [MS05]. Jedoch, es gilt ebenso ein bis heute gültiger Rechtsgrundsatz von hoher Bedeutung, der besagt *audiatur et altera pars*, d.h. *man muss auch die Gegenseite hören*.[2] Die demokratische Gesellschaftsordnung wiederum fußt auf Thomas Hobbes und seiner bemerkenswerten Annahme eines „*Krieges aller gegen alle*“[3] sowie auf dem aktuellen, bis heute unbezweifelten, sicherheitspolitischen Leitspruch der Sicherheitsorgane: *Wenn du den Frieden willst, bereite den Krieg vor.*[4]
Wer also ist die anzuhörende Gegenseite? IT-Sicherheitsforschung und Hackertum sind von *vornherein* keine echten Gegenseiten. *Les extrêmes se touchent*.[5] Es existieren zumindest in einem bestimmten Umfang *fließende* Grenzen, und es stellt sich die Frage, inwieweit sich die Ethik als Instrument zur Beurteilung ethischer Normen innerhalb der IT-Sicherheitsforschung/ Hacken überhaupt anwenden lässt. Das Hauptargument dafür, *keine* ethischen Betrachtungen, wie in den gewohnt-üblichen Diskursen, in den Begrifflichkeiten von „Ethik und Hacken, rsp. „Ethik in der IT-Sicherheitsforschung“ zu führen, ist ein nicht-triviales, da diese all zu schnell einem Werkzeug gleichen, dass sich selbst überprüfen will, – ähnlich einem Streichholz, dass selbst prüfen soll, ob es brennen werden wird. – Wie soll sich ein Instrument kritisieren, wenn es nur sich selbst zur Kritik zu Verfügung hat?
In einem solchen gesellschafts-, macht- und wirtschaftspolitischem vorausgesetzten Szenario kann es leicht dazu kommen, dass „im Krieg die Gesetze schweigen“, und dass quasi das „höchste Recht zu größtem Unrecht“ wird.[6] Die traditionelle Einteilung der Ethik in eine *deskriptive* oder *normative*, also eine Empirische, Beschreibende oder Normenbegründende, Fallanalysen Durchführende greift an diesem Punkt der extremen Annäherung und Überschneidung von „Gut und Böse“ nicht tief genug.
Eine praxisnahe oder Angewandte Ethik zeigt allenfalls, dass man Moral nicht wie das Recht erzwingen kann, noch appellativ einfordern[7], – und selbst das Recht noch beugsam ist. Im globalisierten Kontext von Multikulturalität, Multiperspektivität und multiplen Identitäten gestaltet sich eine Ausarbeitung einer einheitlichen Normen- und Rechtsordnung selbstredend noch schwieriger, wenn nicht sogar unmöglich. Um eventuell ethische Richtlinien erstellen zu können muss unserer Meinung nach, selbst die theoretische Ethik (die sogenannte metaethische) überdacht werden, da die Ethik insgesamt im Kontext der IT-

[1] Das ist ein mittelalterliches Gelehrten Sprichwort, das sich schon bei Luther findet. „Mundus vult decipi, ergo decipiatur.“ Der oftmals verwendete Zusatz „also soll sie betrogen werden“ ist von Paracelcus.
[2] Anm.: Dieser Grundsatz geht auf den antiken Redner Demosthenes (385-322 v. Chr.) zurück.
[3] „Bellum omnium contra omnes“, z.B. in: *Leviathan*, Part 1, Chapter 13, 165; oder: *De Cive*, Praefatio, Section 14.
[4] „Si vis pacem, para bellum“, stammt aus dem 4. Jahrhundert.
[5] „Die (äußersten) Gegensätze berühren sich.“ (Jean de la Bruyère).
[6] Vgl. Cicero: „silent leges inter arma” und „summum jus summa injuria.” In: *Pro Tito Annio Milone ad iudicem oratio.*
[7] Anm.: Selbst der vielzitierte *kategorische Imperativ* von Immanuel Kant ist empirisch nicht mehr als eine Makulatur, wie Nicolai Hartmann richtigerweise begründet: „Sofern das besagt, dass wirklich die jedesmalige ‚Maxime’ der Handlung ihre Richtschnur daran hat, ob sie zugleich allgemeines Gesetz sein könnte oder nicht, so liegt darin offenkundig etwas, was der Mensch als Persönlichkeit nicht prinzipiell wollen kann. Er muss vielmehr zugleich wollen, dass über alle Allgemeingültigkeit hinaus noch etwas Eigenes in seinem Verhalten sei, was an seiner Stelle kein Anderer tun sollte oder dürfte. Verzichtet er darauf, so ist er eine bloße Nummer in der Menge, durch jeden Anderen ersetzbar; seine persönliche Existenz ist vergeblich, sinnlos.“ [Har49].
Diese Feststellung und Problematik betrifft ebenso die diversen, von der UN oder OECD herausgegebenen Richtlinien, wie z.B. die „OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html,
„UNO Guidlelines Concerning Computerized Personal Data Files“,
http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm

Sicherheitsforschung/ Hacken in *partieller Selbsterkenntnis* verhaftet bleiben muss. Eine Umwertung der Werte, d.h. ein Perspektivenwechsel ist nötig, um den engen Rahmen aufzusprengen, bzw. die Gefahr der Selbstreferenziellität und der Schwarz-Weiß Malerei in den Diskursen zu mindern. Die rein ethische Diskussion führt in eine Sackgasse und eventuell an der (langfristig zukunftsfähigen) Sach- und Problemlage vorbei, da sie schlicht zu kurz greift.
Wir werden im Folgenden von der vordergründig ethischen Diskussion wegführen und aufzeigen, dass und warum es sich in der IT-Sicherheitsforschung und dem Hackertum im Grunde genommen *nicht* um ethische Probleme handelt, sondern die ethischen Fragen auf *ästhetische Fragen* zurückführen.
Durch diese Umwertung wollen wir mit dazu beitragen nachhaltigen Lösungsansätze zu finden und aus dieser anderen Perspektive heraus zu einer konstruktiven Diskussion, um den Begriff der Verantwortungszuschreibung beizutragen, und einen vergrößerten Horizont an Lösungen im zukünftigen Feld der Ethikkodizes aufzeigen. Unsere Ausführungen werden auf unterschiedlichen Denkebenen fundiert, auf der theoretischen als auch der praktischen Ebenen.
Nicht näher eingegangen wird auf den komplexen Begriff der ethischen Verantwortung, wie er in den ‚alten' Debatten, die bis heute aufgrund ihrer vielfältigen Ambivalenzen ungelöst sind, anzutreffen ist, sondern es sei auf Hans Lenk [LM91, Len99, Len08] verwiesen, der in seinen Theorien ebenso konkrete Fallbeispiele aus allen Branchen analysiert sowie differenziert auf die Dimensionalität der Individual-, Institutionen-, Kooperationen-verantwortlichkeit u.v.m. eingeht. Wir werden statt dessen direkt *in media res* gehen und uns mit der allgemeingültigen Feststellung begnügen, dass der Verantwortungsbegriff immer „Konstruktionscharakter" hat und „relational" ist. [Len99]. Er ist ein sozialer und idealisierter Zuschreibungsbegriff, der mit unterschiedlichsten Erwartungshandlungen, Verteilungs-problemen, Bewertungen und Interpretationen behaftet ist.
Das Besondere an dem Gebiet der IT-Sicherheit ist, im Gegensatz zu anderen Wissenschaften, ihre von *vornherein bestehende*, inhärente, fließende Grenze der Moral, ihre gleichzeitige Doppelgesichtigkeit von „Gut und Böse", nicht erst ihre sporadische und/ oder nachträgliche Verantwortlichkeitsbestimmung (z.B. Chemieunfall etc.). Diese Doppelgesichtigkeit gilt es zu hinterfragen.

3. Sozialpsychologischer Ansatz: Pragmatisches Hacken

Die hervorstechendeste Eigenschaft innerhalb der IT-Security, verglichen mit anderen Disziplinen, ist der Aspekt der Sicherheit, d.h. die Verteidigung vor Bedrohungen. Der wesentliche Unterschied zwischen der IT-Security und anderen Security-Bereichen besteht darin, dass der Gegner automatisiert ist, sowie schnell und unsichtbar für das menschliche Auge. Insbesondere möchten wir nachdrücklich darauf hinweisen, dass fast alle Sicherheitsprobleme auf menschlichen Interessenkonflikten basieren. Allgemein, ohne einen existierenden Angreifer könnte man die IT unbedenklich ohne jegliche Sicherheitsmaßnahmen benützen.
Von daher liegt das Hauptaugenmerk der Verteidigungsstrategien auf der menschlichen Intelligenz. Neben dem Beherrschen von strategischem und analytischem Denken sind unverzichtbare Fähigkeiten für IT-Sicherheits-Spezialisten die *Antizipation, Empathie, Flexibilität, Adaption* und ein *hohes Kreativitätspotential.*

Diese Fähigkeiten helfen jedoch nicht nur dem Verteidiger, der sein Potential nicht auf einmal voll ausspielt und etwas in der Hinterhand behält, um sein System am Laufen zu halten[8], sondern ebenfalls dem Angreifer des Systems. Wichtig dabei ist, dass defensives oder aggressives Reagieren als jeweils *eine* mögliche Antwortmöglichkeit auf *ein und denselben* Vorgang erfolgen kann. Die Angemessenheit liegt im kontextuellen Ermessungs- und Interpretations*spielraum.*
Bemerkenswert ist dazu, wie Jochen-Thomas Werner in einer Polizei-Veröffentlichung zur inneren Sicherheit den idealen Mitarbeiter von Ordnungsagenturen charakterisiert, um gesellschaftliche Risiken zu minimieren [Wer02]:

„Vier Dinge [...] können einem handelnden Menschen zum Verhängnis werden:
- seine Neigung alles, was schwarz auf weiß geschrieben steht, für wahr zu halten.
- Sein starres Festhalten an überkommenen und unreflektierten und (von ihm) nicht begründbaren Wissensfragmenten.
- Sein Glaube, im Beruf immer rational handeln zu müssen.
- Seine Vorstellung, dass gleiche Ursachen gleiche Wirkungen hervorrufen.“ (S.14)

Er begründet dies damit, dass „Wirklichkeit fortwährend erzeugt wird“ und, dass es „eine, gemeinsam von allen Menschen geteilte Welt nicht gibt. [...] sie bewohnen unterschiedlichste soziokulturellen Universen.“ (S. 7f)
Diese Festestellung erkannte bereits der Technikphilosoph José Ortega y Gasset bei der Beantwortung seiner Frage ‚Was ist die Technik’ in aller seiner Konsequenz und Deutlichkeit: „Der Mensch ist ein Programm, daher ist er das, was er noch nicht ist, sondern was er sein möchte. [...] ein Anspruch. [...], weil das Sein des Menschen nicht gegeben, sondern zunächst nur eine eingebildete Möglichkeit ist, ist die menschliche Gattung von einer Unbeständigkeit und Wandelbarkeit, die sich mit den tierischen Gattungen nicht vergleichen lässt. Kurz die Menschen sind ungeheuer ungleich, im Gegensatz zu dem, was die Gleichmacher der letzten Jahrhunderte und die Rückständigen der Gegenwart sagen.“ (S. 51-55). Eine Nichtbeachtung dieser Erkenntnis führt bei Ortega y Gasset unweigerlich zu einem ‚Aufstand der Massen’.[9] Die Kernaussage ist, dass der Mensch, und zwar jeder einzelne, für sich das Maß aller Dinge ist. Die damit einhergehende Selbstverständlichkeit besteht in den per se gegebenen unterschiedlichen Handlungsweisen, die als eine wertneutrale, unethische Tatsache hingenommen werden sollten. Werner favorisiert von daher gesehen zurecht den Sicherheitsgedanken, dass man in einer mehrdimensionalen Welt „eine Reziprozität der Perspektiven entwickeln können“ müsse. (S. 10).
Die IT-Security basiert, wie die Aktivität des Hackings essentiell auf der *menschlichen Komponente* innerhalb der Technologie, bzw. des Technikgeschehens; – einem Faktum, das lange Zeit von unserer von Rationalität und Aufklärung bestimmten Gesellschaft verdrängt wurde. Dies wird nicht nur eindrucksvoll von einer der mächtigsten Hacking-Techniken, dem *Social Engineering* demonstriert, sondern auch durch die Tatsache, dass die erfolgreichsten Angriffe auf IT-Systeme immer auf der elementaren Stufe der menschlichen Unvollkommenheit durchführbar sind. Darüber hinaus ist dies die erkennbare Spitze eines Eisberges einer *allgemeinen* gesellschaftlichen *Technikentwicklung*, die sich zukünftig nicht länger aufhalten lassen wird.
Der Anspruch und die einzigartige Situation der IT-Security besteht in der Kombination von zwei Extremen: die größtmöglichsten Gegensätzlichkeiten, in ihrer Wechselwirkung, nämlich die (logisierte) Technik mit dem (unlogischen, unergründlichen) Humanum, zu vereinen.

[8] Anm.: Ein gutes Beispiel ist das Autofahren, bei dem man durch eine rücksichtsvolle Fahrweise zugunsten der eigenen und der Gesamtsicherheit, gelegentlich auf die einem selbst zustehenden Verkehrsordnungsregeln, verzichtet.
[9] Anm.: s. sein bekanntes Buch: *Der Aufstand der Massen*.

Dies rechtfertigt eine Sonderstellung der ‚IT-Sicherheit' innerhalb der Wissenschaften. Dadurch wird die IT-Sicherheit/ das Hacken (im Idealfall) zur *realistischsten* Wissenschaft unter den Wissenschaften.[10]
Dies zeigt sich wiederum auch und gerade an der technologischen Komplexität, die ein Hauptgrund für eine Reihe von Sicherheitsproblemen darstellt, d.h. ohne die Komplexität der heutigen Computersysteme gäbe es keine Sicherheitsfragen.[11]
Der sozial relevante Punkt der Sicherheit, die Gefahrenabwehr, wird durch die Erfassung von Gegensätzlichkeiten, des Perspektivismus und der Mehrdeutigkeiten gewährleistet, anders formuliert, anthropologische Technik-Forschung muss nicht nur defensiv, sondern auch offensiv angelegt sein, und ihr „Alleinstellungsmerkmal" unter den (meisten) Wissenschaften[12] wäre die *Offenheit* in ihren *Voraussetzungen* und *Randbedingungen*.
Alle diese gegensätzlichsten und unterschiedlichsten Denk-, Handlungs- u. Emotionsweisen zu vereinen, erfordert die größtmögliche *Freiheit* und *Kreativität.* Das ist aufgrund der Spannbreite zuallererst kein ethischer Vorgang, – er befindet sich sozusagen *Jenseits von Gut und Böse* –, wenngleich er nachgeschaltet mit Moral zu tun haben kann, quasi perspektivisch gestückelt und ‚etikettiert' wird.[13]

4. Kunstvolles Hacken

Der Sprung raus aus der Ethik führt hinein in die Ästhetik, **–** und in die Kunst. Wir werden jedoch keine computergenerierte Kunst, Fraktale, ASCII-Kunst etc. betrachten, sondern die *Struktur der Informatik an sich,* bzw. der IT-Sicherheit. Auf dieser theoretischen Ebene wird die pragmatische Vorgehensweise der IT-Sicherheit als auch des des Hackens eindeutig als eine Handlung ‚Jenseits von Gut und Böse' fundiert.
Als das Curriculum der Informatik ursprünglich erstellt wurde, verortete man, wie z.B. der Informatiker Friedrich L. Bauer[14], die Informatik als „Ingenieur-Geisteswissenschaft (oder als Geistes-Ingenieurwissenschaft, wem das besser gefällt.)" [Bau74]. Doch, was für ein Gebilde soll das sein?
Die IT ist eine angewandte Wissenschaft und es werden Dinge geschaffen, in diesem Sinne ist sie den Ingenieurswissenschaften verwandt. Das Geschaffene ist andererseits immateriell, – wie man konkret an den Haftungsfragen bestens ablesen kann.[15] Es gibt einen jedoch wichtigen Unterschied zwischen den Ingenieur- oder auch den Naturwissenschaften und der

[10] Anm.: Dies wollen im Grunde genommen ja alle Wissenschaften, allein das Vermögen fehlt, also zieht man sich auf die Idealisierung und die Beschränkung von ‚realen' und ‚funktionierenden' Teilbereichen zurück.
[11] Anm.: Kürzlich konnte bewiesen werden, dass der erste Operating System Kernel korrekt ist. Die Arbeit betrug 30 Mannjahre für 7.500 Codezeilen. Siehe z.B.:
http://www.theengineer.co.uk/Articles/312631/Safer+software.htm
[12] Anm.: Lediglich die Philosophie zieht gleich oder übertrifft sogar in ihrer breit angelegten Offenheit die IT-Sicherheit: In der Philosophie muss man mit einer Art *offenen Einkreisung* operieren, da man nicht weiß, welches ihr Gegenstand, resp., im analogischen Fachjargon der IT-Sicherheit gesprochen, ihr indirekter Gegner, ist. Dieser Gegner ist jedoch noch facettenreicher, – und man hat noch nicht einmal die Gewähr ihn erkennen zu können.
[13] Anm.: Man bemerke, dass man an dem extremsten Punkt der Annäherung von ‚Gut' und ‚Böse' gleichfalls beim *humanistischen Bildungsideal* angelangt ist, dass ebenso eine ethisch-kulturelle Höchstentfaltung der menschlichen Kräfte fordert. Doch an diesem Punkt kippt die Moral, – nicht in Amoralität, sondern in die Ästhetik –, da er in letzter Konsequenz bedeutet: „Tout comprendre, c'est tout pardonner", (Alles verstehen heißt alles verzeihen), bzw. korrekter und sinnvoller heißt der ursprüngliche Satz von Germaine de Staël: „Tout comprendre rend très indulgent" (Alles verstehen macht sehr nachsichtig). Eine Haltung, die in der westlich-römischen Rechtsprechung Eingang gefunden hat.
[14] Anm.: Einer der Mitgründer der Programmiersprache ALGOL, geb.1929.
[15] Anm: Haftungsfragen werden in der IT recht originell gelöst, wie man in jeder EULA (End-User Licence Agreement) nachlesen kann: die Softwarehersteller garantieren niemals und für nichts. Das könnten sich andere Branchen gar nicht leisten.

IT-Security: deren Aufgabe besteht hauptsächlich darin ‚versteckte' Gesetze zu finden, d.h. physikalische Gesetze aufzustellen und diese adäquat umzusetzen. Der wissenschaftliche Fortschritt verläuft entlang dieser Marschroute. Es ist in den Ingenieur- und Naturwissenschaften unmöglich neue Gesetzlichkeiten zu formulieren, die sich konträr zu den Naturgesetzen verhalten oder eine Ingenieurleistung entgegen dem Diktat der Natur zu vollbringen. Auf der anderen Seite ist es in der IT-Security ohne Weiteres möglich auf vielfältige Weise Problemlösungen zu erarbeiten, die alle gleichzeitig falsch und richtig sein können.
Ingenieur- und Naturwissenschaften haben von daher so etwas wie einen utopischen, egalisierenden Charakter[16], während die IT-Security – ähnlich den Geisteswissenschaften – durch einen prozessualen Charakter charakterisiert wird. Mehr Übereinstimmungen findet man zwischen der IT-Security und der Philosophie, wenn man sich den Arbeitsprozess an nicht-trivialen Softwareprogrammen verdeutlicht:

1. Hier gibt es keine Möglichkeit, die Qualität von Software zu messen, genauer gesagt: man kann überhaupt *nichts* bei Software *messen*.
2. Jegliche gefühlte Kontrolle über den Entwicklungsprozess von Softwareprojekten ist Illusion (sobald es über Zeiträume von mehr als 4 Wochen geht).
3. Software wird nie fertig.
4. Die Intentionen von Software-Erschaffern werden von den Konsumenten oft falsch interpretiert und das Produkt wird zweckentfremdet genutzt.
5. Programmierung von allen nicht trivialen Systemen ist kein Handwerk, sondern Design (möglicherweise auch Architektur).

Man kann in dieser Aufzählung ohne Weiteres die Worte ‚Software' und ‚Programmierung' durch ‚Philosophie', oder im Vorgriff, durch ‚Kunst' ersetzen und erhält einen sachlich richtigen Text. Hier ist die Verbindung der IT(-Security) zum Menschen hergestellt. Der Mensch ‚an sich' kann als ein unfertiges, komplexes, offenes (self-modifying) Programm betrachtet werden. Ein Moment der *Unbestimmtheit* ist somit diesen Techniken, insbesondere der IT-Security, sowie den Geisteswissenschaft immer innewohnend.

Wenn man sich alle diese Charakterisierungen vor Augen hält, kann man dann nicht die IT-Sicherheit, bzw. das Hacken aus ihrem Zwitterzustand herausholen und sinnvoll irgendwo anders verorten?
Wenn Informatiker weder Ingenieure noch Geisteswissenschaftler sind, kann und sollte man ihnen eine Art *Künstler-Status* zusprechen, – und damit konsequenterweise auch dieselben *Freiheiten.* Das bedeutet ganz konkret: die *Kunstfreiheit* anzuwenden.
Die Kunst ist ganz allgemein ein Gebiet, das sich selbst immer wieder übertrifft, d.h. indem in vielerlei Hinsichten ständig Grenzen überwunden werden. Im Falle der IT-Sicherheit, bzw. des Hackens werden vielfältige Grenzen überwunden, – dies ist geradezu eine *notwendige Grundvoraussetzung* ihrer Arbeit. Wir sind außerdem der festen Überzeugung, dass in der Regel die Fähigkeit Grenzen überwinden zu können, zugleich mit einschließt, dass man sich der Grenze gegenwärtig ist, da die Arbeit an und mit ihr das Bewusstsein für die Grenzlinie schärft. Diese Fähigkeit ist durchaus der eines professionellen Kampfsportlers vergleichbar, der nicht nur darin ausgebildet ist Menschen zu verletzen, sondern, da er besser als der Durchschnitt um die Verletzlichkeit weiß, kann er den Einsatz und die Wahl seiner ‚grenzüberschreitenden' aggressiven Mittel der Situation angemessener einsetzen.

[16] Anm.: Einprägsam und einfach formuliert: es gibt veraltete Sicherheitskonzepte, aber keine wirklich veralteten naturwissenschaftlichen Gesetze, d.h. ihre formulierbare Modifizierbarkeit hält sich in gewissen vorgegebenen Grenzen.

Die Kunst und die Informatik arbeiten explorativ und multi-dimensional.[17] Die Kunst darf provozieren und alle öffentlichen Moralvorstellungen beleidigen, ohne großartig zur Rechenschaft gezogen zu werden. Im Gegenteil, Kunst soll und muss provozieren. Die Hacker müssen, um neue Sichtweise generieren zu können, ebenfalls „provozieren", d.h. Werte umwerten und perspektivisch arbeiten. Das Suchen von Fragen, von Lücken bzw. Verwundbarkeiten und Antworten ist ein wesentliches Charakteristikum.
An dieser Stelle wird nochmals ganz deutlich, warum ethische Diskussionen im Bereich der IT-Sicherheit keinen Sinn ergeben, genauso wenig wie im Bereich der Kunst. Die größte Ähnlichkeit zur Kunst ergibt sich aus den großen Freiheiten, die man in der Informatik hat, verglichen mit anderen (Ingenieurs-)wissenschaften, d.h. die Freiheit ein System auf so viele unterschiedliche Weisen zu bauen, wobei nicht zuletzt auch ein persönlicher *Stil* entscheidet, und es, wie in der Kunst, auch keine Metrik gibt, die besagt, welche die bessere Lösung ist, oder auch: die schönere. Unter Informatikern ist es Usus über die Schönheit von Lösungen zu sprechen. Der Rekurs auf den persönlichen *Stil* weist über die Kunst hinaus auf den größeren Horizont der *Ästhetik,* – und nicht auf die Ethik.
Um überhaupt den Anforderungen gewachsen zu mit den unterschiedlichsten und gegensätzlichsten menschlichen Denkweisen umzugehen, ist es unverzichtbar die größtmögliche Freiheit und Kreativität zu haben. Dies ist gemäß dem Bedeutungsumfang und der Vielfältigkeit der Aufgabe keine Frage von moralisch-ethischen Betrachtungen, sondern es ist ‚Jenseits von Gut und Böse' – obgleich es manchmal moralisch verurteilt wird.
Vor diesem Hintergrund wird klar, dass *der Krieg der Vater aller Dinge ist*[18], wie Heraklit schon wusste. Ähnlich verhält es sich in der Philosophie und der heutigen Kunst, wo Meinungsverschiedenheiten die Grundlage aller Diskussionen und denkerischen Entwicklungen bilden. Der gleiche Umstand greift in der IT-Sicherheit, wo der Konflikt von Meinungen der tatsächliche Hintergrund von IT-Sicherheitslücken ist. In allen genannten Fällen sind die Gegensätzen und Widersprüchen unverzichtbare Bedingungen, aus denen neue schöpferische Perspektiven und integrierende Einsichten erwachsen.
Mit der ‚Gefährlichkeit' der IT-Securiuty, bzw. dem Hacken verhält es sich im Grunde genommen wie mit der ‚Gefährlichkeit' der Philosophie, sprich der *Gedankenfreiheit,* oder der ‚Gefährlichkeit' der Kunst, also der *Kunstfreiheit*. Alle drei basieren sozusagen zuallererst auf einem *individuellen, immateriellen Schöpfungsprozess*.

5. Schlussbetrachtung

In dem bekannten Text *The Conscience of a Hacker* [Bla86], besser bekannt als *Hacker's Manifesto* lässt sich das angesprochene Dilemma zu einem guten Teil auflösen, wenn man erkennt, dass es sich *nicht* nur um eine ethische Problematik handelt, – sondern im Wesentlichen um eine *ästhetische*.
Selbst die Rechtslage für die IT-Sicherheitsindustrie lässt sich vor diesem diskutierten Hintergrund und mit dem Aspekt des *„Künstler-Status"* sinnvoll modifizieren und erweitern.
Das Gewissen eines Hackers ist in Grunde genommen seine strikte *gewissen*hafte Arbeitsweise, – die er professionell zum Wohle der Gesellschaft erbringt. Auf dieser Art ist er während seiner Arbeit *zugleich* der Teufel *und* der Ritter des Daten-Highways, beziehungsweise das Gewissen der (Entwicklung) von Wissen und Erkenntnis, – weil jede große Erkenntnis Janusköpfig ist.

[17] Anm.: Die Philosophie arbeitet genauso, sie ist jedoch *nicht primär* auf Maschinen, bzw. Materialien fokussiert. Die Naturwissenschaften sind dagegen eher progressiv/ linear ausgerichtet.
[18] „Polemos panton pater." Heraklit, B53.

Literaturverzeichnis

[Bau74] Friedrich L. Bauer, *Was heißt und was ist Informatik*? In: (Hg. Michael Otte), *Mathematiker über Mathematik*, Springer, Berlin 1974, S. 357.

[Bla86] Llyod Blankenship. *The Conscience of a Hacker,* January 8 1986, originally published at *Phrack*, Vol. One, Issue 7, Phil 3 of 10.

[Har49] Nicolai Hartmann, *Ethik,* 1949.

[Len99] Hans Lenk, *Praxisnahes Philosophieren*, Stuttgart 1999, S.106.

[Len08] Hans Lenk, *Zur Verantwortung des Ingenieurs*. In: (Hg. Matthias Maring) *Verantwortung in Technik und Ökonomie*, Karlsruhe 2008.

[LM91] Hans Lenk, Matthias Maring, (Hg.) Technikverantwortung. Güterabwägung – Risikobewertung – Verhaltenskodizes, Frankfurt 1991.

[MS05] Kevin D. Mitnick und William L. Simon. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers.* Wiley, December 2005.

[Wer02] Jochen-Thomas Werner, *Netzwerk innere Sicherheit*. In: http:// www. polizei-newsletter.de/documents/innereSicherheit.pdf, 2002.

[yG49] José Ortega y Gasset, *Betrachtungen über die Technik*, Stuttgart, 1949.