

>»computergestützte Identifikation«<

>Orwell 2011: Amerika auf dem Weg in einen allgegenwärtigen Überwachungsstaat – Biometrie, Gesichtserkennung und »computergestützte Identifikation«

Tom Burghardt

2006 [enthüllte der frühere AT&T-Techniker Marc Klein](#), dass die großen amerikanischen Telekommunikationskonzerne mit der Regierung kooperierten, um amerikanische Bürgerinnen und Bürger auszuspionieren. Seither hat kein Bericht auf den Punkt gebracht, dass wir uns einer furchteinflößenden Phalanx unsichtbarer Gegner gegenübersehen: den Sicherheits- und Nachrichtendienstfirmen, die die dunkle Seite des Nationalen Sicherheitsstaates ausmachen.

Die Wogen der Enthüllungen des vergangenen Monats durch die »Internet-Guerillas« [Anonymous](#) sind noch nicht abgeebbt, und die von Hackern im Internet veröffentlichten E-Mails und andere Dokumente der amerikanischen Sicherheitsfirma [HBGary](#) liefern frappierende Erkenntnisse darüber, wie wenig Transparenz in Bezug auf die Zusammenarbeit zwischen Privatunternehmen und der Regierung existiert.

Die jüngste Front in dem anhaltenden Krieg gegen Bürgerrechte, Datenschutz und den Schutz der Privatsphäre betrifft das Interesse des Pentagon an sogenannter »Persona Management Software«. Ein Euphemismus für komplexe Computerprogramme, mit denen es Militärangehörigen oder Mitarbeitern von Unternehmen – wie man will – möglich sein soll, zahlreiche Avatars oder »fiktive Identitäten« im Internet zu steuern. Unsere modernen Schattenkrieger hoffen auf diese Weise, sich gegenüber ihren Widersachern im »Krieg der Ideen« mithilfe verdeckter Propagandakampagnen, die als Verbreitung von Informationen ausgegeben werden, einen Vorteil zu verschaffen.

Ein allgegenwärtiger Überwachungsstaat

Überall finden sich heute Anzeichen für einen allmächtigen Überwachungsstaat. Diese reichen von sogenannten »persistenten Cookies« (das sind dauerhaft gespeicherten Daten, die über den Computernutzer hinterlegt werden), die alle unsere Schritte im Internet nachverfolgen, bis hin zur Indizierung von Dissidenten, die bereits »vorbeugend« in öffentlichen und privaten Datensammlungen »inhaftiert« sind:

Noch nie war unsere Freiheit, unsere Meinung ohne Angst vor Einschüchterungen oder Schlimmeren so stark bedroht.

Der Verfassungsrechtler [Jack Balkin erklärte](#), die Umwandlung des Staates von einer demokratischen Republik auf der Grundlage rechtsstaatlicher Normen in einen »nationalen Überwachungsstaat« sei durch »hohe Investitionen in elektronische Überwachungstechnologien und andere Mechanismen zur Umgehung traditioneller Schutzvorschriften für die in der Verfassung garantierten, unveräußerlichen Grundrechte und vorgeschriebenen Verfahrensweisen gekennzeichnet ... Zu diesen Umgehungsmechanismen gehören die Zusammenarbeit zwischen Privatunternehmen und öffentlichen Stellen bei der Überwachung und dem Austausch von Informationen, die Ausweitung der Auffassungen und Bestimmungen zu Staatsgeheimnissen [unter

>»computergestützte Identifikation«<

dem Vorwand der Gefährdung der nationalen Sicherheit], die Ausweitung von Durchsuchungsanordnungen und der sogenannten National Security Letters (einer strafbewehrten behördlichen Anordnung zur Übergabe von Dokumenten oder Informationen), ein System der Sicherheitsverwahrung, eine Ausweitung der Nutzung von Militärgefängnissen, außerordentliche Auslieferungen [von Verdächtigen] an andere Länder und aggressive Verhörtechniken, die sich außerhalb der Grenzen des herkömmlichen Kriegsrechtes bewegen.«

Die Aushöhlung der Bürgerrechte geht weiter, wie selbst das [Wall Street Journal](#) in der vergangenen Woche berichtete. Diesem zufolge hatte die Regierung Obama, die unter dem Motto »Veränderung« angetreten war, neue Bestimmungen verabschiedet, die es Ermittlern erlauben, »Verdächtige, denen Terroranschläge in den USA vorgeworfen werden, länger als andere festzuhalten, ohne dass sie über ihr Recht auf Aussageverweigerung und anwaltlichen Beistand während der Verhöre informiert werden müssen. Damit werden die Ausnahmen von Bestimmungen, die seit mehr als 40 Jahren die Behandlung und das Verfahren gegenüber eines Verbrechens verdächtiger Personen regelten, massiv ausgeweitet.« Die Zeitung verweist darauf, dass diese Revision seit langer Zeit bestehender Bestimmungen und Rechtsprechung »eine weitere Abkehr von der noch vor der Präsidentschaftswahl vorgebrachten Kritik [Obamas] an unorthodoxen Methoden der Terrorbekämpfung bedeutet«.

Ebenfalls in der vergangenen Woche enthüllte die Internetseite [The Raw Story](#), das FBI habe mit den Planungen »für ein Biometrie-Projekt mit einem Umfang von einer Milliarde Dollar und für den Bau einer modernen biometrischen Einrichtung begonnen, die gemeinsam mit dem Verteidigungsministerium betrieben werden soll«. Das neue FBI-Biometriezentrum, von dem ein Teil bereits in Clarksburg im US-Bundesstaat West-Virginia arbeitet, »soll auf der Grundlage eines Systems aufgebaut werden, das vom Rüstungskonzern Lockheed Martin entwickelt wird«.

Zunächst auf der Grundlage von Fingerabdrücken, so The Raw Story weiter, soll das Zentrum »als weltweite Datenbank für Strafverfolgungsbehörden dienen und den Austausch biometrischer Bilder und Daten ermöglichen«. Nach seiner Vollendung soll »das System nach außen erweitert werden und möglicherweise auch elektronische Gesichtserkennung und andere moderne Formen computergestützter Identifikation umfassen«.

Die Umwandlung des FBI in eine politische Behörde zur Verbrechensverhinderung [durch vorausseilende umfassende Datensammlung] wird noch durch andere Maßnahmen vorangetrieben. So wurden Polizeiwachen auf bundesstaatlicher und regionaler Ebene mit elektronischen Fingerabdruck-Scannern ausgestattet, die es ihnen ermöglichen, von jedem Verdächtigen Fingerabdrücke zu nehmen, selbst wenn diese weder verhaftet noch wegen eines Verbrechens verurteilt wurden. In seinem Buch [Cities under Siege \(zu Deutsch: Belagerte Städte\)](#) warnt Stephen Graham:

»Unter Bedingungen wie diesen entwickelt sich sehr rasch eine Sichtweise der westlichen Sicherheits- und Militärdoktrin, die die juristische und operationelle Trennung zwischen Polizei, Nachrichtendiensten und dem Militär sowie die Unterscheidung zwischen Krieg und Frieden und zwischen Operationen auf lokaler, nationaler und globaler Ebene verschwimmen lässt.«

>>computergestützte Identifikation«<

Dieser prekäre Stand der Dinge, so betont Graham, führt dazu, dass sich unter den Bedingungen einer globalen Wirtschaftskrise sowohl im vermeintlich demokratischen Westen, als auch an den Rändern der sogenannten Dritten Welt »Kriege und damit verbundene Mobilisierungen zeitlich und räumlich kaum mehr begrenzen lassen«.

Unter solchen Umständen bedeutet die berüchtigte Erklärung Dick Cheneys, der Krieg gegen den Terror könne möglicherweise Jahrzehnte andauern, eigentlich, so Graham, dass »die sich abzeichnende Sicherheitspolitik sich auf die Erstellung von Profilen von Einzelpersonen, Örtlichkeiten, von Verhalten, von Vereinigungen und Gruppen stützt«. Aber um die Erstellung dieser Profile effektiver zu gestalten, sei es nun in Kairo, Kabul oder New York, halten es Funktionäre staatlicher Sicherheitsdienste und ihre privaten Partner für geboten, immer größere Datenmengen aus dem Überwachungssystem herauszufiltern, das ohnehin schon durch eine Überfülle an »Situationsbewusstsein und - einschätzungen« überladen ist.

»Im vergangenen Oktober«, berichtete die Internetseite [Secrecy News](#), »legte der Direktor Nationale Nachrichtendienste (DNI) offen, dem National Intelligence Program (NIP) hätten im Haushaltsjahr 2010 53,1 Mrd. Dollar zur Verfügung gestanden. Und der Verteidigungsminister erklärte, für die Arbeit des Military Intelligence Program (MIP) hätte der Haushalt 2010 27,0 Mrd. Dollar bereitgestellt. Zum ersten Mal wurden damit überhaupt Zahlen zum MIP-Haushalt vorgelegt. Insgesamt umfasste der Haushalt für Nachrichtendienste im Haushaltsjahr 2010 damit 80,1 Mrd. Dollar.« Darin sind natürlich die schwarzen Kassen der CIA und des Pentagon noch gar nicht enthalten, in denen eine Vielzahl hochgeheimer und verdeckter Programme unter einer schwindelerregenden Fülle von Decknamen und Abkürzungen versteckt sind. Im Februar dieses Jahres enthüllte die Internetseite [Wired](#), die Gesamtsumme dieser Geheimhaushalte belaufe sich »wie schon im vergangenen Jahr auf etwa 56 Mrd. Dollar«, aber auch bei dieser Zahl könne es sich nur »um die Spitze des Eisbergs geheimer Finanzierung handeln«.

Es liegt auf der Hand, dass solche Aufwendungen in Zeiten massiver wirtschaftlicher und sozialer Angriffe auf die Arbeiterklasse einen Skandal darstellen, weniger offensichtlich aber sind die Mittel, die von der sogenannten »Geheimdienst-Community« (dem von Ronald Reagan 1981 per Dekret gegründete Zusammenschluss von 16 Geheimdiensten der USA) eingesetzt werden, um ein von Ausbeutung und Korruption durchsetztes, unhaltbare System aufrecht zu erhalten.

Das bringt uns wieder zum Hackerangriff auf HBGary zurück.

Operation MetalGear

Die Medien haben sich zurecht auf die Berichterstattung über die schmierige Kampagne konzentriert, die der Bank of America und der amerikanischen Handelskammer von der hochkarätig besetzten Anwaltskanzlei und Lobbygruppe Hunton & Willams (H&W) vorgeschlagen worden war und die darauf abzielte, WikiLeaks und Kritiker der Handelskammer mundtot zu machen. Aber die als Fundgrube zu bezeichnende Menge an E-Mails, die von Anonymous gehackt und ins Netz gestellt wurden, enthüllen zahlreiche Pentagon-Programme, die direkt gegen den Kern unserer Kommunikationsfreiheit gerichtet sind.

>»computergestützte Identifikation«<

Die Internetzeitung [The Tech Herald](#) berichtete, die Unternehmen Palantir Technologies und Berico Technologies versuchten zwar, zu HBGary und Hunton & Williams auf Distanz zu gehen, »aber im Jahr 2005 gehörte Palantir zu den zahllosen Unternehmensgründungen, die von der CIA über [In-Q-Tel](#), ihr Frontunternehmen zur Anschubfinanzierung [von Tarnfirmen], ins Leben gerufen worden waren«. Der Journalist Steve Ragan schrieb dazu:

»Bei ihren Investitionen konzentrierte sich In-Q-Tel auf Unternehmen, die sich auf die automatisierte Sammlung und Verarbeitung von Informationen spezialisiert hatten.« Mit anderen Worten: Palantir und Dutzende andere Unternehmensgründungen aus dem Sicherheitsbereich mit einem Volumen von 200 Mio. Dollar erhielten über CIA-Risikokapitalanleger-Frontunternehmen Steuergelder für die Entwicklung von Produkten, die man sowohl zivil als auch militärisch nutzen konnte. The Tech Herald enthüllte: »Palantir Technologies war das »Zugpferd«, wenn es um die Aktivitäten von »Team Themis« ging.« [Team Themis ist ein Sammelbegriff für Geheimdienstfirmen der Regierung.]

In Vorschlägen, die an H&W übermittelt worden waren – einem Unternehmen übrigens, das der Bank of Amerika von einem Experten des Justizministeriums empfohlen worden war –, »erklärte Team Themis, man wolle »das erhebliche Wissen über die Entwicklungen und Datenintegrations-Umgebungen Palantirs weitergeben, damit alle gesammelten Daten »nahtlos in den Analyserahmen Palantirs integriert werden können, um die Analyse von Links und Objekten auszuweiten«.

Nach dem Coup mit HBGary Federal und dem Mutterunternehmen HBGary enthüllte Anonymous das anhaltende Interesse und Vertragsangebote zwischen diesen Unternehmen, Booz Allen Hamilton und der amerikanischen Luftwaffe im Zusammenhang mit der Entwicklung von Computerprogrammen, die es »Internetkriegern« ermöglichen, fiktive Identitäten zu schaffen, um so dem Pentagon Manipulationen in sozialen Internetnetzwerken wie Facebook, Twitter und in Internetblogs zu gestatten.

Ragan verweist darauf, dass »das Konzept einer solchen Technologie nicht neu« sei, und »Methoden zur Erfassung und Steuerung von Ansehen und Identitäten [im Internet] schon seit Jahren von der Regierung und der Privatwirtschaft genutzt werden«, die jüngsten Enthüllungen seien aber deshalb so beunruhigend, weil es sich hier offensichtlich um Pläne geheimer staatlicher Einrichtungen handle, diese Computerprogramme für Propagandakampagnen zu nutzen, mit deren Hilfe man sowohl die amerikanische als auch die Öffentlichkeit eines anderen Landes leicht beeinflussen könne.

Weder HBGary, noch Booz Allen konnten sich entsprechende Verträge sichern, aber das Interesse des in Ungnade gefallenen früheren Vorstandschefs von HBGary Federal, Aaron Barr, und anderer, die Anforderungen eines Militärstaates zu bedienen, wird dafür sorgen, dass die Entwicklung weiter vorangetrieben wird. Anonymous erklärte, dieses Programm trage den Codenamen »[MetalGear](#)«, und ist überzeugt, dass zu diesem Programm »eine Armee fiktiver Internet-Identitäten gehört, die die Internetseiten sozialer Netzwerke unterwandern, um die Bevölkerung in Scharen über scheinbar von etablierten Online-Gemeinschaften (wie etwa Facebook) verbreitete Informationen zu manipulieren. Darüber hinaus könnte die Identität bisher anonymer Personen über den Abgleich gespeicherter Informationen aus zahlreichen Quellen aufgedeckt

>»computergestützte Identifikation«<

werden, indem man Verbindungen zwischen separaten Internetkonten ermittelt und diese Informationen dann dazu benutzt, Dissidenten und Aktivisten zu verhaften, die im Schutz der Anonymität arbeiteten.«

Wie sich die Leser erinnern werden, ging es genau um Technologien wie diese, die es, wie Aaron Barr prahlte, Strafverfolgungsbehörden erlaubten, gegen Anonymous vorzugehen und die Identität von WikiLeaks-Informanten und -Unterstützern aufzudecken.

Aus einer Ausschreibung (RTB220610), die auf der Regierung-Internetseite FedBizOpps.Gov in bester Orwellscher Manier unter der Rubrik »Unterstützung für das Gesetz zur Informationsfreiheit« veröffentlicht wurde, geht hervor, dass »die Luftwaffe Computerprogramme sucht, die zehn Identitäten pro Nutzer erlauben, wobei jede dieser fiktiven Identitäten mit einem eigenen biografischen und sozialen Hintergrund, individuellen Details und einer Internetpräsenz ausgestattet sein muss, die in technischer, kultureller und geografisch [sic] Hinsicht widerspruchsfrei sein soll«.

Darüber hinaus, so sagt man uns, soll es »diese individuelle Anwendung dem Operator erlauben, zahlreiche verschiedene Internet-Identitäten vom gleichen Computer aus und ohne befürchten zu müssen, durch erfahrene Gegner enttarnt zu werden, zu führen«. Beunruhigenderweise sollen »diese Identitäten praktisch überall auf der Welt über normale Internetbetreiber und soziale Netzwerke auftauchen und angemeldet werden können. Zu den Dienstleistungen gehört eine nutzerfreundliche Anwendungsumgebung, um das Situationsbewusstsein und die Lagebewertung des Nutzers dadurch zu maximieren, dass man in Echtzeit lokale Informationen abbildet.«

Um ein Höchstmaß an Geheimhaltung zu sichern, heißt es in der Ausschreibung, müsse in der Lizenz die Identität der Regierungsbehörden und Unternehmensorganisationen geschützt werden. »Unternehmensorganisation« ist ein Euphemismus für private Unternehmer, die von der Regierung unter Vertrag genommen werden, um die Drecksarbeit zu erledigen.

In der Ausschreibung wird präzisiert, dass die lizenzierte Software es »den Organisationen [ermöglichen soll], ihre auf Dauer angelegten Internet-Identitäten durch die Zuweisung statischer IP-Adressen zu jeder Identität zu verwalten. Einzelpersonen können statische Personifikationen darstellen, was ihnen erlaubt, über einen längeren Zeitraum als die gleiche Person zu erscheinen. Zugleich ermöglicht dies Organisationen, unter häufiger Verwendung unterschiedlicher IP-Adressen die gleiche Internetseite zu besuchen oder gleiche Internetdienste in Anspruch zu nehmen, was den Eindruck eines normalen Nutzers und nicht den einer Organisation erweckt.«

Barrs voreiliges Herausposaunen hat möglicherweise Team Themis diese Operation vermässelt, aber man fragt sich, wie viele ähnliche Operationen weiterhin aus den schwarzen Kassen des Verteidigungsministeriums finanziert werden und weiterlaufen.

Unternehmens-Einblicke

Nach den Enthüllungen des vergangenen Monats meldete die britische Tageszeitung [The Guardian](http://TheGuardian) nun, dass ein »kalifornisches Unternehmen einen Vertrag mit dem Zentralkommando (CENTCOM) der amerikanischen Streitkräfte,

>»computergestützte Identifikation«<

das die Operationen der US-Armee im Nahen und Mittleren Osten sowie Zentralasien leitet, abschließen konnte. Dabei ging es um die Entwicklung eines Computerprogramms zum »Online Persona Management«, das es einem oder einer Angehörigen der US-Armee erlauben würde, bis zu zehn separate Internet-Identitäten zu kontrollieren, die weltweit verortet sein könnten.«
Bei dem Unternehmen handelt es sich um eine mysteriöse Firma aus Los Angeles mit Namen Ntrepid, über die sich auf ihrer Unternehmensinternetseite kaum Informationen finden lassen, auch wenn dort im Firmenprofil behauptet wird, die Firma beliefere Behörden aus den Bereichen nationale Sicherheit und Strafverfolgung mit Computerprogrammen, Hardware und Steuerungsdienstleistungen für Internetoperationen, analytische und linguistische Zwecke sowie das Erfassen und Nachverfolgen.

Nach Angaben der Guardian-Journalisten Nick Fielding und Ian Cobain umfasst der Vertrag mit CENTCOM ein Volumen von 2,76 Mio. Dollar. CENTCOM wollte sich nicht dazu äußern, ob dieses Multi-Persona-Projekt bereits in Betrieb genommen wurde, und auch keine Stellungnahme zu möglichen anderen, ähnlich gelagerten Verträgen abgeben.

Wie um die Hintermänner des Unternehmens noch unschärfer erscheinen zu lassen, enthüllte [The Tech Herald](#), Ntrepid sei vermutlich nur ein »Geisterunternehmen«, ein 100-prozentiges Tochterunternehmen der [Cubic Corporation](#). Dieses Unternehmen mit Sitz in San Diego beschreibt sich selbst als einen »Weltmarktführer bei Rüstungs- und Verkehrssystemen und Dienstleistungen«, das sich jetzt auch als »internationaler Lieferant in den Bereichen Chipkarten und RFID-Lösungen« positioniere. [Unter RFID (»radio-frequency identification«) versteht man die »Identifizierung mithilfe elektromagnetischer Wellen, die die Erkennung und Lokalisierung von Gegenständen, aber auch von Lebewesen ermöglichen soll.] Auf der Liste auf der Internetseite Washington Technology rangiert Cubic auf Platz 75 der [führenden Vertragspartner der Regierung im Jahr 2010](#).

Der Gründer des Unternehmens, Walter J. Zable, ist heute noch Vorstandsvorsitzender. Cubic gilt als eines der ältesten und größten Unternehmen für Rüstungselektronik an der Westküste. Das Unternehmen verfügt über zahlreiche hochrangige Verbindungen zu konservativen Republikanern wie Darrell Issa, Duncan Hunter und Dan Coates. Im Rahmen der Wahlen 2010 spendete das Cubic-Management an die 90.000 Dollar an republikanische Kandidaten. Rund 20.000 Dollar davon gingen nach Angaben des Center for Responsive Politics auf seiner Internetseite [OpenSecrets.org](#) an den Fraktionsvorsitz der Republikaner im Kongress und weitere 30.000 Dollar an den Fraktionsvorsitz der Republikaner im Senat.

Im Jahr 2009 betrugen die Einnahmen des Unternehmens etwa eine Milliarde Dollar, wobei der größte Teil der Zusammenarbeit mit dem Verteidigungsministerium entsprang. Die Abteilung »Internetlösungen« liefert dabei »spezielle Produkte und Lösungen für den Bereich Internetsicherheit für Kunden aus den Bereichen Rüstung, Nachrichtendienste und Heimatschutz«. Ragan berichtet, die Ausschreibung der Luftwaffe, die von der Internetgruppe Anonymous veröffentlicht worden war, »richtete sich an das Unternehmen Anonymizer, das 2008 von der Abraxas Corporation, einem Unternehmen, das eng mit Nachrichtendiensten zusammenarbeitet, aufgekauft wurde. Als Grund wurde angegeben, dass Anonymizer bereits über entsprechende

>»computergestützte Identifikation«<

Computerprogramme sowie Kenntnisse und Erfahrungen im Bereich der Persona Management Software verfügte«. Später wurde Abraxas für 124 Millionen Dollar von Cubic geschluckt. Diese Erwerbung wurde von Washington Technology als der seit Jahren »beste Deal im nachrichtendienstlichen Bereich« gewertet.

Wie The Tech Herald berichtet, verließen »einige der führenden Talente von Anonymizer, das später von Abraxas aufgekauft wurde, die Muttergesellschaft Cubic, um ein eigenes Unternehmen im Nachrichtendienst-Umfeld aufzubauen. Sie werden heute als Mitglieder der Führungsriege bei Ntrepid aufgeführt, das schließlich aus dem Rennen um den 2,7 Mio. Dollar schweren Regierungsauftrag als Gewinner hervorging.«

Damit entsteht Raum für Spekulationen, da »im Eintrag im Unternehmensregister Ntrepids Abraxas früherer Vorstandschef und Gründer Richard Helms als Direktor und Vorstandsmitglied sowie der ehemalige Finanzvorstand Wesley Husted als Vorstandsmitglied aufgeführt sind. Das neue Unternehmen ist also möglicherweise wenig mehr als eine Strohfirma für Cubic, die den Blicken der Öffentlichkeit entzogen ist.

Zu den »[Sicherheitsdienstleistungen](#)«, die von dem Unternehmen angeboten werden, heißt es: »Tochterunternehmen von Cubic arbeiten sowohl selbstständig als auch in Kooperation, um vielfältige und breit gefächerte Lösungen für Sicherheitsprobleme zu entwickeln«. Dazu gehören »C4ISR [wird vom amerikanischen Militär als Abkürzung für die englischen Begriffe für die Bereiche >Kommando, Kontrolle, Kommunikation, Computer, nachrichtendienstliche Komponenten, Überwachung und Aufklärung< verwandt] -Datenverbindungen für Heimatschutz-Operationen in den Bereichen Nachrichtendienst, Überwachung und Erkundung«, ein virtuelles Analysezentrum Cubics, das verspricht, »überlegene Situationsbewertungen für Entscheidungsträger in Regierung, Industrie und gemeinnützigen Organisationen« bereitzustellen, Analysen menschlicher Verhaltensmuster sowie andere Bereiche, nach denen es Sicherheitsfanatiker verlangt.

Der Guardian berichtet, »der Vertrag im Zusammenhang mit den >Vielfach-Identitäten< soll im Rahmen eines Programmes mit dem Namen Operation Earnest Voice (OEV) vergeben worden sein, das zunächst als Mittel psychologischer Kriegsführung gegen die Internet-Präsenz von Al-Qaida-Unterstützern für den Einsatz im Irak entwickelt wurde«. Aber seit damals, schreiben Fielding und Cobain weiter, »wurde OEV zu einem mit 200 Mio. Dollar ausgestatteten Programm ausgeweitet und soll gegen Dschihadisten in Pakistan, Afghanistan und dem Nahen Osten eingesetzt werden«.

Der damalige CENTCOM-Kommandeur General David Petraeus erklärte zwar im vergangenen Jahr vor dem Streitkräfteausschuss des Senats, das Programm solle »extremistischer Ideologie und Propaganda entgegenwirken«, aber angesichts der Enthüllungen im Zusammenhang mit HBGary ist die Frage wohl gestattet, ob Unternehmen, die an dem verleumderischen und illegalen Vorgehen gegen WikiLeaks beteiligt waren, bereits Versionen einer »Persona Management Software« entwickelt haben, die gegen innenpolitische Widersacher eingesetzt werden könnte.

Wir können nicht mit Sicherheit sagen, ob dies der Fall ist, aber angesichts der Tatsache, dass Projekte oder Operationen etwa aus anderen Bereichen des

>»computergestützte Identifikation«<

»Krieges gegen den Terror« manchmal schleichend aus dem Ruder laufen, wie etwa das unbefugte Abhören von Telefonen durch die NSA und Spionageoperationen des Verteidigungsministeriums gegen Kriegsgegner, die auch als Projekte »öffentlich-privater Partnerschaft« zwischen Sicherheitsfirmen und geheimen staatlichen Strukturen abgewickelt werden, sollte damit Schluss sein.<

Quelle: <http://info.kopp-verlag.de/hintergruende/geostrategie/tom-burghardt/orwell-2-11-amerika-auf-dem-weg-in-einen-allgegenwaertigen-ueberwachungsstaat-biometrie-gesichts.html>