Bei der *Bewaffnung* geht es darum, Waffen und unbemannte Plattformen aufeinander abzustimmen, spezifische Waffen und neue Munition für unbemannte Systeme zu entwickeln und perspektivisch auch Waffen auf der Basis der Nanotechnologie zur Verfügung zu stellen. Es wird davon ausgegangen, dass die Weiterentwicklung der Bewaffnung davon abhängt, ob die vorgenannten Technologien zum Durchbruch gebracht werden.

Auch wenn die Analyse der militärischen Wünsche an Wissenschaft und Technik viel vertiefter und detaillierter durchgeführt werden müsste, um verlässliche Schlussfolgerungen zu treffen, zeichnet sich auch schon bei einer ersten flüchtigen Sichtung ab, dass insbesondere von der Informatik viel erwartet wird. Als Forschungsgebiete der Informatik sind vor allem Datenfusion, Big Data, cyberphysikalische Systeme, sichere Systeme, Robotik, Künstliche Intelligenz und Autonome Systeme gefordert. Sind das nicht auch genau die Gebiet
gerade mit immensen Finanzmit
den? Ein Schelm, der Böses dab
ist, wäre interessant zu untersuch
1950er- bis 1980er-Jahren der mi
lung der Informatik maßgeblich bestimmt, oder ob das Militär sich einfach die aktuellen Hervorbringungen der zivil emanzipierten Informatik zunutze und zu eigen macht.



*A BAE Raven during flight testing, Brigadier Lance Mans, Deputy Director, NATO Special Operations Coordination Centre*

*erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de*

reitet sich die Bundeswehr vor? Welche Flugzeuge werden nicht über eine Flugabwehr verfügen, sodass Drohnen überhaupt dort fliegen können?

### Was will die Bundeswehr mit Kampfdrohnen?

Waffentragende Drohnen werden bisher und vor allem für gezielte Tötungen, *signature strikes* und unter Inkaufnahme vieler Ziviltoter eingesetzt, sodass mit ihnen in den meisten Einsatzfällen Kriegsverbrechen begangen werden. Will die Bundeswehr auch solche Kriegsverbrechen begehen können? Wenn JA, wo soll das zukünftig geschehen? Welche Feinde Deutschlands sollen so bekämpft werden? Was hätte das mit dem Verteidigungsauftrag der Bundeswehr zu tun? Wenn NEIN, was sonst? Aus politischen und militärischen Kreisen hört man dazu oft litaneiartig wiederholt: Die Kampfdrohnen sollen dem Schutz der Soldaten bzw. dem Schutz von Feldlagern dienen. An welche zukünftigen Feldlager in welchen Ländern der Welt ist dabei gedacht?

### Hoffnung

Trotz der vielen Gegenbeispiele habe ich die Hoffnung nicht aufgegeben, dass Menschen vernünftig denken und handeln können, und dass sich insbesondere in einer Demokratie die Vernunft bei politischen Entscheidungen durchsetzen kann. Bezogen auf die Entwicklung unbemannter Waffensysteme hoffe ich, dass sich Informatikerinnen und Informatiker wo und wie immer möglich diesem Irrsinn verweigern. Bezogen auf bewaffnungsfähige Drohnen hoffe ich, dass die deutsche Regierung auf ihre Beschaffung und Neuentwicklung verzichtet, weil die immensen notwendigen Finanzmittel besser verwendet werden können, weil diese Waffen keinen Verteidigungsbedarf decken, weil diese Waffensysteme mit oder ohne Autonomie unüberwindliche ethische Probleme aufwerfen.

**Daniel Leisegang**

# Der cyber-militärische Komplex

## Die dunkle Seite des Silicon Valley

*Den Begriff „militärisch-industrieller Komplex" prägte US-Präsident Dwight D. Eisenhower vor gut 50 Jahren. Er beschrieb damit eine Entwicklung, in der die Rüstungsindustrie durch den Zweiten Weltkrieg und im Zuge des Kalten Krieges erheblich an Einfluss auf die politischen Entscheidungen in Washington gewann. Die technische Entwicklung ist seither rasant fortgeschritten; es sind vollständig neue Technikfelder entstanden, in aller Regel mit erheblichem militärischen oder Dual-Use-Potenzial. Im digitalen Bereich, im „Cyberraum", ist die Verknüpfung von Militär und Industrie besonders eng, wie der Autor hier an zahlreichen Beispielen aufzeigt.*

Das Silicon Valley gilt als die postindustrielle Innovationsschmiede der USA. Die dort angesiedelten IT- und Hightech-Unternehmen sind überzeugt, dass ihre *smarten* Produkte selbst die kompliziertesten Probleme des Alltags lösen können. Und in der Tat: Apples iPhone hat die Kommunikation von Millionen Menschen geradezu revolutioniert. Facebook verbindet über 1,3 Milliarden Menschen miteinander, derweil Google nicht weniger als sämtliche Fragen der Menschheit beantworten will.

Doch das sonnige Tal südlich von San Francisco steht nicht nur im Dienst der guten Sache, sondern ist bereits seit Jahrzehnten auch Teil des militärisch-industriellen Komplexes der USA. Die

enge Zusammenarbeit zwischen Nachrichtendiensten, der US-Armee und den IT-Unternehmen lässt die Trennlinie zwischen militärischen Anwendungen auf der einen und zivilen Produkten auf der anderen Seite mehr und mehr verschwimmen. Die Ursache dafür liegt nicht zuletzt in der zunehmenden Verbreitung des Internets und der Digitalisierung unserer Kommunikation.

## Electronic Warfare: Die Entstehung des Silicon Valley

Die Verbindungen zwischen dem Silicon Valley und dem US-amerikanischen Militär reichen bis weit in die erste Hälfte des vergangenen Jahrhunderts zurück. Eine wichtige Rolle spielte dabei die Stanford University. Sie liegt etwa 60 Kilometer südöstlich von San Francisco nahe der Kleinstadt Palo Alto. Bereits in den 1930er-Jahren ermunterten die dort lehrenden Professoren ihre Studenten, in der näheren Umgebung Unternehmen zu gründen. Aus diesen ging unter anderem der Weltkonzern Hewlett-Packard hervor: Er wurde 1939 in einer Garage in Palo Alto ins Leben gerufen. Diese Garage gilt heute als die eigentliche Geburtsstätte des Silicon Valley.

Die wirtschaftliche Entwicklung der Region gewann 1951 an Fahrt. Damals wurde der Grundstein für den *Stanford Industrial Park* gelegt, den weltweit ersten Industriepark, der auf die Erforschung und die Produktion technologischer Produkte spezialisiert war. Der Park gehörte damals der Universität Stanford; heute ist er unter anderem Sitz des Facebook-Hauptquartiers.

Für die Herausbildung des Silicon Valley spielte *Frederick Terman* eine entscheidende Rolle. Der Professor für Ingenieurwissenschaften gilt – neben dem Physiker und Nobelpreisträger *William Bradford Shockley* – als einer der beiden Begründer des IT-Standorts.

Terman genoss in den 1930er-Jahren den Ruf, einer der besten Funktechniker der Vereinigten Staaten zu sein. Während des Zweiten Weltkrieges leitete er das streng geheime Electronic Warfare Lab an der Harvard University. Terman sollte erforschen, wie sich das deutsche Radarsystem effektiv stören ließ, um so Verluste auf Seiten der alliierten Luftstreitkräfte zu reduzieren.

Nach dem Krieg kehrte Terman 1946 an die Stanford University zurück. Er verfolgte das Ziel, das dortige Ingenieurinstitut zu einem weltweit anerkannten Zentrum für Mikrowellen- und Elektrotechnik zu machen, und gründete das Electronics Research Lab (ERL). Das ERL wurde von Beginn an auch vom US-Militär finanziert; im Gegenzug nutzte die Armee dessen Erkenntnisse während des Kalten Krieges, um die Sowjetunion auszuspionieren.[1]

Das ERL war jedoch nicht das einzige Labor in Stanford, das im Dienste der US-Armee stand. Auch die Forschungsergebnisse des Applied Electronics Lab (AEL), das sich der Störung von Radarsignalen und der elektronischen Aufklärung verschrieben hatte, wurden militärisch genutzt – vor allem während des Vietnamkriegs. Im April 1969 besetzten allerdings Studenten das Labor und verlangten dessen Schließung – mit Erfolg.

Einige der Forscher wechselten daraufhin in die Privatwirtschaft und gründeten rund um Palo Alto Start-ups, die sich auf Mikrowellen- und Radartechnik spezialisierten. Damit bestärkten sie zum einen den Aufstieg des Silicon Valley als IT-Standort. Zugleich festigten sie die Zusammenarbeit der dortigen Unternehmen mit dem Militär und den amerikanischen Geheimdiensten.

## Google: Verwurzelt im militärisch-industriellen Komplex

Die Kooperationen zwischen dem Silicon Valley und der US-Regierung in Washington D.C. bestehen bis heute fort. Auch der Internetkonzern Google ist im Bereich der Militärforschung aktiv – ungeachtet seines inoffiziellen Firmenmottos „Don't be evil".

Google Inc. wurde 1998 von den Informatikern *Larry Page* und *Sergey Brin* gegründet. Bereits deren Forschungsprojekt an der Stanford University, aus dem der Konzern hervorging, wurde unter anderem von der Defense Advanced Research Projects Agency (DARPA) finanziert.[2] DARPA besteht seit 1958 und soll als Forschungsbehörde des US-Verteidigungsministeriums die „technische Überlegenheit des US-Militärs aufrechterhalten".

Nach der Unternehmensgründung arbeitete Google eng mit dem amerikanischen Auslandsgeheimdienst National Security Agency (NSA) und der National Geospatial-Intelligence Agency (NGA) zusammen, der zentralen US-Behörde für militärische und geheimdienstliche kartografische Aufklärung.

Im Jahr 2003 stattete Google die NSA beispielsweise intern für mehr als zwei Mio. US$ mit seiner Suchtechnologie aus. Zwar verlängerte die NSA den Vertrag nach einem Jahr nicht, dennoch stellte Google dem Nachrichtendienst seine Suchwerkzeuge noch ein weiteres Jahr zur Verfügung – ohne dies in Rechnung zu stellen. 2004 beauftragte auch die Central Intelligence Agency (CIA) Google, den Nachrichtendienst intern mit seiner Suchtechnologie auszustatten.[3]

Zudem bietet Google verschiedenen US-Geheimdiensten und dem Militär *geospatial intelligence services* an.[4] Bei diesen handelt es sich im Kern um *raumbezogene Aufklärungsdienste*,[5] welche die Kartenanwendung *Google Earth* nutzen. Insbesondere die NGA nutzt diese, um geografische Daten mit Geheimdienstinformationen anzureichern und zu visualisieren, und unterstützt damit, so Google, unter anderem die US-Regierung im Bereich der Sicherheitspolitik.[6]

## Von Keyhole zu Google Earth

Auch Googles Kartentechnologie wurde maßgeblich von den Geheimdiensten finanziert. Google Earth ging aus den Produkten des Start-ups Keyhole hervor. Keyhole wurde 1990 gegründet und hatte sich frühzeitig auf dreidimensionale Kartentechnologie spezialisiert. Als dem Unternehmen 2001 die Insolvenz drohte, half ihm *In-Q-Tel* mit einer Finanzspritze aus der Not.

In-Q-Tel (IQT) war 1999 von der CIA gegründet worden und fungiert als dessen Capital-Venture-Arm. Das „Q" im Namen steht für die fiktive Forschungsabteilung des britischen Geheim-

dienstes MI6 in der James-Bond-Reihe, die dessen Agenten mit Armbanduhrenlaser und explodierenden Schlüsselringen versorgt. IQT verfolgt das Ziel, in neue Technologien zu investieren, die sich kurzfristig für geheimdienstliche oder militärische Zwecke einsetzen lassen. Bislang hat IQT mehr als 3,5 Mrd. US$ in ausgewählte IT-Unternehmen gesteckt. Auf Regierungsseite kooperiert das Unternehmen mit der Defense Intelligence Agency (DIA), dem US-Heimatschutzministerium sowie der NGA. Die Mittel des Unternehmens stammen allerdings in der Regel aus dem Haushalt der CIA.[7]

Die finanzielle Rettung von Keyhole zahlte sich aus: Die CIA und die NGA wirkten im Anschluss gezielt darauf hin, dass die Produkte von Keyhole an militärische und geheimdienstliche Zwecke angepasst wurden. Die Kartentechnologie unterstützte die US-Armee unter anderem bei der Invasion des Irak ab dem Jahre 2003.

Im Jahr 2004 kaufte Google Keyhole und nutzte dessen Technologie, um seinen eigenen dreidimensionalen Kartendienst Google Earth zu entwickeln. Gleichzeitig setzte Google die Kooperation mit den Nachrichtendiensten wie auch mit dem US-Militär fort. Die CIA macht aus der Zusammenarbeit keinen Hehl: Auf ihrer Website beschreibt sie Google Earth als „CIA-unterstützte Technologie".

Die Kooperation mit der NGA baute Google im Jahr 2008 sogar aus: Gemeinsam schickten sie einen Beobachtungssatelliten ins All – den *GeoEye-1*. Dieser galt damals als der kommerzielle Beobachtungssatellit mit der höchsten Bildauflösung: Täglich erfasst er eine Fläche doppelt so groß wie die Bundesrepublik. Google darf diese Aufnahmen verwerten, jedoch nur in einer reduzierten Auflösung. Zwei Jahre danach ging Google eine „formelle Beziehung zum Informationsaustausch" mit der NSA ein. Der Geheimdienst sollte dem Konzern dabei helfen, einen ausgeklügelten Angriff chinesischer Hacker auf dessen Dateninfrastruktur aufzuklären.[8] Welche Inhalte Google in diesem Rahmen mit der NSA austauschte, unterliegt bis heute der Geheimhaltung.

## Google-Manager mit militärischen Erfahrungen

Die enge Bindung Googles an den militärisch-industriellen Komplex[9] spiegelt sich auch in der Unternehmensführung wider. Eine Reihe von Google-Managern kommt aus dem US-Militär oder hat zuvor für Nachrichtendienste gearbeitet.

*Michele R. Weslander Quaid* zum Beispiel ist seit 2011 Googles *Innovation Evangelist* und technische Leiterin der Google-Abteilung, die für öffentliche Aufträge zuständig ist. Das *Entrepreneur Magazine* zählte sie im vergangenen Jahr zu einer der sieben mächtigsten Frauen der Welt. Der Zeitschrift gegenüber beschrieb Weslander Quaid ihre Tätigkeit als „Brückenbauerin" zwischen dem Silicon Valley und den Regierungsbehörden in Washington. Dabei kommt der Google-Managerin zugute, dass sie zuvor unter anderem bei der NGA, dem Direktor der nationalen Nachrichtendienste, dem Nationalen Aufklärungsamt sowie dem US-Verteidigungsministerium tätig war.

*Shannon Sullivan* hingegen leitet bei Google die Abteilung für Verteidigung und Aufklärung. (Sein offizieller Titel lautet *Head of Defense & Intelligence*.) Er ist dafür zuständig, Google-Dienste für das Verteidigungsministerium bereitzustellen. So hatte eines von Sullivans Projekten zum Ziel, 50.000 US-Soldaten mit angepassten Google-Applikationen auszustatten.[10] Zuvor hatte Sullivan über zwei Jahrzehnte bei der *U.S. Air Force* gearbeitet – unter anderem in der Geheimdienstabteilung.

## Kriegsroboter im Dienste der Kunden?

Google hilft jedoch nicht nur bei der Auswertung von Daten, sondern ist seit Kurzem auch im Robotergeschäft unterwegs. 2013 kaufte der Konzern in nur sechs Monaten acht Roboterfirmen auf, darunter Boston Dynamics. Das Unternehmen wurde 1992 von *Marc Raibert* gegründet, einem ehemaligen Professor am Massachusetts Institute of Technology (MIT); Raibert gilt in den Vereinigten Staaten als *Vater* der Laufroboter. Boston Dynamics hatte vor allem im Auftrag des US-Militärs gearbeitet, und nach der Firmenübernahme sicherte Google zu, die bestehenden Verträge zu erfüllen. Mit dem Unternehmen hat Google nicht nur 80 Ingenieure und Wissenschaftler *eingekauft*. Zudem verfügt der Internetkonzern nun über den weltschnellsten Laufroboter, genannt *Cheetah* (Gepard). Dieser hat vier Beine, erreicht eine Geschwindigkeit von knapp 47 Stundenkilometern und ist damit etwas schneller als der mehrfache Olympiasieger über 100 Meter, *Usain Bolt.*

Der Bau, der Verkauf und der Einsatz von Robotern ist ohne Frage ein großer Zukunftsmarkt, insbesondere im Bereich der Automatisierung und der Erforschung künstlicher Intelligenz. Welche Ziele Google allerdings genau mit dem Kauf der Roboterfirmen verfolgt, ist derzeit noch offen.

## Drohnen: Der Wettkampf um den Luftraum

Klarer sind die Ziele bei der Entwicklung unbemannter Flugzeuge erkennbar. Anfang 2014 erwarb Google den Drohnenhersteller Titan Aerospace. Das Unternehmen stellt riesige, solarbetriebene Flugzeuge her. Diese können mehr als drei Millionen Flugkilometer zurücklegen, bevor sie wieder landen müssen. Aus einer Höhe von 30 Kilometern sollen sie weltweit unwegsame Gebiete mit Internetzugang versorgen.

In diesem Bereich bewegt sich insbesondere Facebook in direkter Konkurrenz zu Google. Die *Social Community* übernahm den britischen Drohnenentwickler *Ascenta* und plant ebenfalls den Bau tausender Flugdrohnen. Diese sollen die Spannweite von Jumbo-Jets haben und, so der Plan, vier Milliarden Menschen mit drahtlosem Internetzugang versorgen.[11]

Ein weiterer Konzern – allerdings mit Sitz in Seattle – interessiert sich ebenfalls für Drohnen: Amazon. Der Internethändler möchte die unbemannten Fluggeräte nutzen, um Bestellungen an die Kunden auszuliefern. Bisher stehen diese Pläne noch am Anfang, allerdings ist das Vorhaben gewiss mehr als ein reiner Marketing-Gag: Für sein Vorhaben hat Amazon unter anderem Ingenieure der NASA und der *U.S. Navy* abgeworben: *Neil Woodward* leitet seit April 2014 die Abteilung, die für Testflüge und Zertifizierungen zuständig ist; zuvor war er NASA-Astronaut und Navy-Flugoffizier. *Mark Sibon* ist seit September 2014

*Operations Program Manager* bei Prime Air. Davor leitete er drei Jahre lang bei der US-Navy die Abteilung Unmanned Aerial Vehicle (Unbemannte Flugkörper).

## Die CIA in der Amazon-Cloud

Nicht nur zur Armee, auch zu den US-Geheimdiensten pflegt Amazon enge geschäftliche Beziehungen. Seit Jahren nutzen über 300 amerikanische Regierungsbehörden, darunter das US-Finanzministerium, die so genannte *GovCloud*. Diese ist Teil der *Amazon Web Services*, mit denen Unternehmen wie auch Privatkunden Speicherplatz auf den Amazon-Servern nutzen können. Im Juli 2013 – und damit inmitten der NSA-Enthüllungen – gab der Konzern bekannt, ausgerechnet von der CIA den Zuschlag für einen Großauftrag erhalten zu haben: Für die Dauer von vier Jahren stellt Amazon dem Auslandsgeheimdienst der USA ein eigens auf sie zugeschnittenes Cloud-Computing-System bereit – Kostenpunkt: mehr als 600 Mio. US$.

Durch diese einträgliche Public Private Partnership befindet sich Amazon in großer wirtschaftlicher Abhängigkeit von der CIA und der US-Regierung. Möglichen Forderungen, Einblicke in die Amazon-Kundendaten oder gar eine direkte Schnittstelle zu den Unternehmensservern zu erhalten, wird sich der Online-Händler wohl kaum entziehen können, ohne gleichzeitig Gefahr zu laufen, eine Reihe wichtiger Großkunden zu verlieren.

## Die Suche nach der Nadel im Big-Data-Heuhaufen

Weitaus weniger bekannt als Google, Facebook oder Amazon ist das ebenfalls im Silicon Valley beheimatete Unternehmen Palantir Technologies. Palantir verfügt über keine direkte Konsumentenbindung, sondern unterhält vor allem Geschäftsbeziehungen zum US-Militär – und zur CIA.

Wie kaum ein anderes Unternehmen des Silicon Valley ist Palantir ein technisch-militärischer Hybrid: Zur einen Hälfte ist das Unternehmen in Washington angesiedelt, zur anderen in Palo Alto.[12] Gegründet wurde es 2004 von dem heutigen Geschäftsführer *Alex Karp* und dem PayPal-Gründer *Peter Thiel*. Thiel investierte gut 28 Mio. US$ in Palantir, weitere zwei Millionen kamen von In-Q-Tel. Heute ist das einstige Start-up eines der am schnellsten wachsenden Unternehmen im Silicon Valley; sein Marktwert wird derzeit auf über acht Mrd. US$ geschätzt.

Der Firmenname leitet sich von den *Sehenden Steinen* aus der Fantasiesaga *Der Herr der Ringe* ab. Dementsprechend hat sich Palantir auf die Entwicklung hochkomplexer Software auf der Grundlage von PayPals Betrugserkennungssoftware spezialisiert. Diese ist in der Lage, verschiedene Datenbanken über einen gemeinsamen Index zu erschließen und deren Inhalt mit menschlicher Sprache abzufragen. Das Suchwerkzeug genießt den Ruf, einfach und intuitiv anwendbar zu sein.

In Geheimdienstkreisen genießt Palantir den Ruf, das effizienteste Werkzeug zu besitzen, um terroristische Netzwerke aufzufinden und zu untersuchen. Dafür prüft und kategorisiert Palantir unterschiedliche Datenquellen – ganz gleich, ob es sich dabei um Namen, Telefonnummern oder Kontobewegungen handelt – und stellt eigenständig Beziehungen zwischen diesen her.[13] Auf diese Weise kann Palantir die sprichwörtliche Nadel im Big-Data-Heuhaufen finden – und bietet damit aus Sicht der Geheimdienste die *Killer-App* schlechthin an.[14]

Die Software wird bislang vor allem im Bereich der militärischen und geheimdienstlichen Aufklärung eingesetzt. So soll Palantir in der Vergangenheit unter anderem Mitglieder eines mexikanischen Drogenkartells ausfindig gemacht haben, nachdem diese einen US-Agenten getötet hatten. Die US-Truppen in Afghanistan hingegen nutzen die Software, um Aufständische aufzuspüren, die mit selbstgebauten Sprengsätzen US-Soldaten töten.[15]

Das Potenzial von Palantir ist damit aber bei Weitem nicht ausgeschöpft. Zu den Beratern des Unternehmens gehören neben der Nationalen Sicherheitsberaterin unter *George W. Bush*, *Condoleezza Rice*, auch der ehemalige CIA-Direktor *George Tenet*. Dieser sagte über Palantirs Software, er wünschte, die CIA hätte ein derart machtvolles Programm vor dem 11. September 2001 besessen. Palantir sei in der Lage, Verbindungen aufzuzeigen, „die fünf, sechs, acht, zehn Jahre zurückreichen". Etwas Vergleichbares habe damals keine Anwendung vermocht.[16]

Daher überrascht es nicht, dass zu Palantirs Kunden neben der CIA längst auch die NSA, das FBI, die Defense Intelligence Agency, das Department of Homeland Security, das National Counterterrorism Center, das U.S. Marine Corps, das U.S. Special Operations Command sowie – nicht zuletzt – die Polizeibehörden in Los Angeles und in New York City gehören.

## Der cyber-militärische Komplex

Dank der voranschreitenden Digitalisierung wird die Zusammenarbeit zwischen dem Silicon Valley und Washington in Zukunft noch enger werden. Denn längst gehen *Big Brother* – die globale Ausspähung durch die US-Geheimdienste – und *Big Data* – die massenhafte Anhäufung von Kommunikationsdaten – Hand

**Daniel Leisegang**

**Daniel Leisegang** ist Politikwissenschaftler und Redakteur bei der Monatszeitschrift *Blätter für deutsche und internationale Politik (blaetter.de)*.

in Hand. Zugleich sind die US-Armee und die Geheimdienste damit auf Analysewerkzeuge angewiesen, die die richtigen Punkte in der schier unendlichen Masse an Informationen finden und miteinander verbinden können.

Fest steht damit auch, dass der cyber-militärische Komplex weiter anwächst – und nach und nach den militärisch-industriellen Komplex ablösen wird, der seine Wurzeln in den 1950er-Jahren hat. Allein in diesem Jahr stehen dem US-Verteidigungsministerium 5,5 Mrd. US$ für Investitionen im Bereich der *Cybersicherheit* zur Verfügung. Ein Großteil davon wird ins sonnige Silicon Valley fließen – und damit in die smarte, neue Überwachungswelt.

Der Beitrag ist in *Wissenschaft & Frieden* 2015-2: *Technikkonflikte, Seite 27–30* erschienen.
*http://wissenschaft-und-frieden.de/seite.php?artikelID=2042*

## Anmerkungen

1 *Steve Blank: The Secret History of Silicon Valley Part VI: Every World War II Movie was Wrong. steveblank.com, 27.4.2009.*
2 *Dazu auch: Nafeez Ahmed: How the CIA made Google. medium.com, 22.1.2015.*
3 *Douglas Edwards (2012): I'm feeling lucky: Confessions of Google Employee Number 59. Boston: Mariner Books.*
4 *Der US-Regierung bietet Google zudem für 6,7 Mio. US$ seine Cloud-basierten E-Maildienste an. Vor diesem Hintergrund ist wenig verwunderlich, dass Länder wie Russland oder China Googles Dienste aussperren; vgl. dazu: Evgeny Morozov: Who's the true enemy of internet freedom – China, Russia, or the US? The Guardian, 3.1.2015.*
5 *Seit 2010 bietet Google der NGA zudem für 27 Mio. US$ „geospatial visualization services" an. Den Auftrag erhielt Google direkt und ohne Ausschreibung, was die NGA damit begründete, dass sie bereits erhebliche Investitionen in die Google-Earth-Technologie getätigt habe, die man nicht verlieren wolle.*
6 *Google Earth Builder supports NGA geospatial efforts. Official Google for Work Blog, 20.4.2011.*
7 *Das Geld, mit dem Keyhole vor der Pleite gerettet wurde, kam allerdings von der NGA. Die NGA verfügt über ein etwa halb so großes Budget wie die NSA; damals gab sie an, das Geld anstelle der »Intelligence Community« zur Verfügung zu stellen.*
8 *Ellen Nakashima: Google to enlist NSA to help it ward off cyberattacks. The Washington Post, 4.2.2010.*
9 *Google arbeitet auch eng mit Rüstungsunternehmen wie Lockheed Martin und Northrop Grumman zusammen. Lockheed erhielt von Google »geospatial technologies«. Northrop zahlte rund eine Million US$ für eine maßgeschneiderte Google-Earth-Anwendung.*
10 *Yasha Levine; The revolving door between Google and the Department of Defense; pando.com, 23.4.2014. Jeremy Scahill: Blackwater for Sale. The Nation, 8.6.2010.*
11 *Derzeit verfügt gerade einmal gut ein Drittel der Weltbevölkerung über einen Zugang zum Internet: Vgl. den Bericht der Internationalen Fernmeldeunion ITU (2014): Measuring the Information Society Report 2014. Genf.*
12 *Daneben unterhält Palantir ein weiteres Dutzend Büros in der ganzen Welt, unter anderem in Tokio, Sydney, Singapur und Tel Aviv.*
13 *Siobhan Gorman: How Team of Geeks Cracked Spy Trade. The Wall Street Journal, 4.9.2009.*
14 *Palantirs Software ist damit das kommerzielle Gegenstück zum NSA-Tool XKeyscore. Mit ihm kombiniert und durchsucht der Geheimdienst Telekommunikationsdaten aus verschiedenen Quellen. Aus diesem Grund sehen Bürgerrechtsorganisationen wie die American Civil Liberties Union in Palantir auch einen „wahren totalitaristischen Albtraum", da die Software es ermögliche, das Leben unschuldiger Amerikaner in nie gekanntem Ausmaß zu überwachen. Andy Greenberg and Ryan Mac: How A »Deviant« Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut. Forbes, 2.9.2013.*
15 *Rowan Scarborough, Military leaders urgently push for new counterterrorism software. The Washington Times, 27.8.2012.*
16 *Ryan Mac: National Security Darling – Why Condoleezza Rice, David Petraeus and George Tenet Back Palantir. forbes.com, 19.8.2013.*



Gertrud Maria Vaske

# Cyberwar – die digitale Front: Ein Angriff auf Freiheit und Demokratie?

## Interview mit Felix *FX* Lindner, Hacker

Felix *FX* Lindner *legte die Energieversorgung der Stadt Ettlingen lahm und hackte Blackberry sowie die Netzwerkstruktur von Cisco. Als ausgewiesener Experte in der Computer-Security-Szene präsentiert „FX" seine Forschungsergebnisse bereits seit über zehn Jahren weltweit auf Konferenzen und macht sie frei im Netz zugänglich. Er ist Gründer, technischer und Forschungsleiter von* Recurity Labs GmbH*, einem Beratungs- und Forschungsunternehmen für IT-Sicherheit im High-End-Bereich, das sich auf Code-Analyse und das Design von sicheren Systemen und Protokollen spezialisiert hat. Das Interview führte* Gertrud Maria Vaske.

**Gertrud Maria Vaske (GMV):** *Was ist Ihrer Meinung nach die größte Bedrohung im Cyberwar? Was war Ihrer Meinung nach die größte Bedrohung für Datensicherheit und Datenschutz im Jahr 2014?*

**Felix *FX* Lindner (FX):** Die größten Bedrohungen erwachsen meiner Meinung nach durch den Mangel an Verständnis bei vielen der verantwortlichen Personen. Dadurch bestimmten in 2013 und 2014 einige wenige Personen das mediale Narrativ und die politische Agenda. Eine sachliche Diskussion über Datensicherheitsstrategien ist leider so selten wie sie dringend angeraten ist.

**GMV:** *Welche Cyberwar-Gefahren gibt es vor allem militärisch, aber auch für die Privatbevölkerung und für Unternehmen?*

**FX:** Das Hauptproblem in allen drei Bereichen ist die blinde Digitalisierungswut. Wir schaffen es nicht, unsere existierenden Computersysteme und Netzwerke abzusichern, bauen aber überall noch mehr und tiefer vernetzte Computer ein, sei das