

Geheimnisvolle Krypto-Offiziere: So kontrollieren 14 Menschen mit sieben Schlüsseln das Internet

9. Februar 2019



Diese Geschichte klingt nach Science-Fiction. Doch sie ist wahr: Das Internet wird von 14 Personen mit sieben physischen Schlüsseln kontrolliert. Diese Schlüsselträger treffen sich viermal pro Jahr für eine Zeremonie wie aus einem Agententhiller.

Ein Hochsicherheitsraum in Los Angeles: Hinter Stahlgittern befinden sich High-Tech-Tresore. Jede Erschütterung schließt die Käfige automatisch. Keine elektronischen Signale gelangen hinein oder hinaus.

Sicherheits- und Reinigungskräften ist der Zutritt streng verboten, wie der britische „[Guardian](#)“ berichtet. Nicht einmal Ethan Hunt, die von Tom Cruise gespielte Hauptfigur der Filmreihe Mission Impossible, könnte hier wohl einbrechen.

Das Telefonbuch des Internets

Die Organisation ICANN (Internet Corporation for Assigned Names and Numbers) hält hier – im Wechsel mit Washington – pro Jahr jeweils zwei so genannte Schlüsselunterzeichnungszeremonien ab, die direkt aus einem Agententhiller stammen könnten. Die mächtige Vereinigung lässt das technische Herz des Internets pumpen.

Internetadressen bestehen aus reinen Zahlenfolgen. Damit man sie sich leichter merken kann, werden sie durch einprägsamere Namen ersetzt. ICANN weist den Namen (z.B. focus.de) einen Nummerncode – die IP-Adresse – zu (z.B. 193.201.12.55). Damit kontrolliert die Vereinigung das „Telefonbuch“ des Internets.

Wer ICANN kontrolliert, kontrolliert das Web

Der Zusammenbruch des Systems würde das Internet ins Chaos stürzen. Bei Eingabe eines Seitennamens in die Suchzeile des Browsers wäre keine Seite mehr aufrufbar.

Noch schlimmer: Wer Zugriff auf die ICANN-Datenbanken bekäme, könnte das System manipulieren und Internetnutzer beispielsweise von echten auf falsche Bankseiten verweisen. Die Folgen wären katastrophal.

Sieben Schlüssel, ein Generalschlüssel

Gleichzeitig muss das System im Fall einer Katastrophe womöglich neu gestartet werden. Dafür gibt es sieben Schlüsselträger, so genannte Krypto-Offiziere. Diese besitzen sieben physische Schlüssel, die Schließfächer ihrer Besitzer auf der ganzen Welt öffnen, wie ICANN in einem Youtube-Video erklärt.

In den Schließfächern lagern Smartcards. Vereint gewähren sie Zugriff auf einen Computer, der wiederum einen digitalen Generalschlüssel generiert – das Passwort der ICANN-Datenbanken.

Gleichzeitig ernannte ICANN sieben Schattenträger. Diese besitzen keine physischen Schlüssel sondern lediglich Smartcards, auf denen Stücke des Codes gespeichert sind.

Zur Sicherheit müssen sie nach Informationen des „Guardian“ einmal pro Jahr ein Bild von sich schicken – mit ihrer Smartcard und einer aktuellen Tageszeitung. Das macht insgesamt 14 Schlüsselträger.

Was passiert bei der Zeremonie?

Seit 2010 kommen die Schlüsselträger viermal pro Jahr zur Erneuerung des Generalschlüssels zusammen, heißt es auf ICANNs Internetseite. Der „Guardian“ durfte dem Ritual im Frühjahr 2014 beiwohnen und berichtet von extremen Sicherheitsvorkehrungen. Der Einlass ins Allerheiligste ist mit einem Augenscanner gesichert.

Im Hochsicherheitsraum folgen die Teilnehmer minutiös dem Protokoll. Darauf sind über 100 Tagesordnungspunkte verzeichnet. Das Ritual wird von mehreren Kameras live ins Internet übertragen.

Die notarielle Sorgfalt hat einen guten Grund. Vor einigen Jahren schrammte das Internet nur knapp an einer Katastrophe vorbei. Damals war ein IT-Spezialist namens Dan Kaminsky auf ein riesiges Sicherheitsleck im DNS-Bereich gestoßen.

Sechs Monate lang arbeiteten Spezialisten der großen Internetfirmen an der Behebung des Internet-GAU. Seitdem geht Sicherheit vor.

Internet unter US-Aufsicht

Das Internet geht auf die US-Regierung zurück: Nach dem Sputnik-Schock 1957 gründete das US-Verteidigungsministerium die Advanced Research Project Agency (ARPA). Diese neutral benannte Agentur sollte die Überlegenheit der technischen Wissenschaften in den USA gegenüber der Sowjetunion wiederherstellen, so argumentierte die Regierung unter dem Ex-Weltkriegsgeneral Dwight Eisenhower.

Im Wesentlichen ging es um die Vorherrschaft im militärischen Kalten Krieg, insbesondere im möglichen Atombomben-Krieg. Hier stieg der Bedarf insbesondere der Air Force an möglichst schneller Beschaffung von Daten der Gegenseite, an Auswertung, Gegen- und Erstreaktion. Es ging um die Beherrschung des Luftraums. Das betraf die beiden Varianten der US-Militärstrategie von der „massiven Vergeltung“ bis zur „flexible response“.

Silicon Valley: Rüstungsindustrie seit dem 2. Weltkrieg

Die technischen Wissenschaften in den USA waren gar nicht unterlegen, bis auf einen engen Ausschnitt der Weltraumforschung. Aber US-Regierung und US-Militär, gemeinsam mit der Rüstungsindustrie, eng verbunden im Militärisch-Industriellen-Komplex (MIK), suchten jeden Anlass, um das nach dem 2. Weltkrieg eingebrochene Rüstungsgeschäft wieder hochzuziehen und die Überlegenheit gegenüber der Sowjetunion auszubauen.

Vor allem in Kalifornien stand die technologische Basis schon bereit. Mit Beginn des 2. Weltkriegs war ein großer Teil der neuen Rüstungsindustrie in das später so genannte Silicon Valley verlegt worden. Die Gegend war klimatisch günstiger als die oft kalte und regnerische Ostküste, und das nur wenig agrarisch genutzte Land konnte schnell bebaut werden – und es gab keine Gewerkschaften.

Zudem lag hier die vom Eisenbahnkönig Leland Stanford gegründete Elite-Universität Stanford. Sie war politisch extrem „konservativ“ und zugleich technologisch innovativ mit einem Schwerpunkt in industriell verwertbaren Wissenschaften. 1939 war in Palo Alto, dem Standort der Universität, der dann lange Zeit größte Computerkonzern des Silicon Valley gegründet worden, Hewlett Packard. 1956 siedelte sich hier der Rüstungskonzern Lockheed im Industriepark der Universität an, um den Bau der neuen Interkontinental-Raketen voranzutreiben, die mit Atombomben bestückt werden konnten.

Neue Generationen von Kampffjets und Bombern wurden produziert. Dafür war eine enorme Menge und Schnelligkeit der Datenverarbeitung nötig. Auch die Großcomputer von IBM brauchten immer leistungsfähigere Chips. Die Halbleiter-Hersteller des Silicon Valley, National Semiconductor, Advanced Micro Devices, Fairchild und Intel wurden schnell zu Großkonzernen.

Hewlett Packard-Chef als Verteidigungsminister

Der größte Teil der von der Pentagon-Agentur ARPA koordinierten Forschung wurde an private Think Tanks vergeben, so an die RAND Corporation, die in Santa Monica/Kalifornien von der Ford Foundation und Douglas Aircraft 1948 gegründet worden war. RAND koordinierte die Forschung an Elite-Universitäten wie Stanford und Massachusetts Institute of Technology (MIT) in Boston.

Die Verbindung von Computer-Industrie und Militär war selbstverständlich. Niemand nahm Anstoß daran, dass David Packard, Mitbegründer und Miteigentümer von Hewlett Packard, während des Vietnam-Kriegs stellvertretender US-Verteidigungsminister unter Präsident Nixon wurde.

1968 gründeten Air Force und Pentagon mit ARPA das ARPANET: Damit sollte unter Leitung des MIT die sichere Datenkommunikation zwischen den vom Pentagon beauftragten Universitäten hergestellt werden. Dafür wurden das Betriebssystem Unix und die Programmiersprache C entwickelt. Der Verteidigungsminister, der ARPANET vorantrieb, war Robert McNamara: Er war zuvor Präsident des Ford-Konzerns, der im 2. Weltkrieg mehr Militärfahrzeuge als Zivildfahrzeuge produzierte, nicht nur für die US-Armee, sondern auch für Hitler-Deutschland.

ARPANET sollte das militärische Gesamtsystem der USA und der NATO datenmäßig vernetzen: Flugzeuge, Flugzeugträger, Luftabwehr, Interkontinentalraketen, Atomsilos, die einzelnen Militärformationen zu Lande, auf dem Meer und in der Luft – einschließlich der Satelliten – und die mehreren hundert um die Erde verteilten Militärstützpunkte, Software und Hardware. Für den Bedarf der US-Militärinterventionen weltweit wurden Methoden der Aufstandsbekämpfung (Counter Insurgency) entwickelt. Ständig wurden wechselnde Gefechtssituationen simuliert. Dafür finanzierte ARPANET auch Forschungen über Verhaltenspsychologie.

ARPANET als militärische Vorstufe des Internet

Das Militär, die auch in der Rüstungsproduktion tätigen Autokonzerne Ford und General Motors, die Pentagon-Auftragnehmer IBM und General Electric sowie die Telefonkonzerne ITT und AT&T waren bis in die 1980er Jahre die Antreiber für die digitale Datenverarbeitung. Am Projekt der Strategic Defence Initiative Organisation (SDIO, Raketenabwehrsystem) von Präsident Ronald Reagan wurden hunderte Subunternehmen beteiligt.

Ähnliches gilt für das Global Positioning System (GPS), dessen Entwicklung an der Johns Hopkins University koordiniert wurde. Wagniskapital-Finanziers und Wall Street-Banken schafften das Kapital für ständige Neugründungen heran. Mitte der 1980er Jahre wurden 1.950 Unternehmen zur High Tech-Branche des Silicon Valley gezählt.

So gehörten zum erweiterten MIK immer mehr zivile Unternehmen wie der Kopiergeräte-Hersteller Xerox, der an der Stanford University für das Militär die grafische Benutzeroberfläche entwickelte (Apple profitierte später davon). Die Telefonkonzerne wie Bell und AT&T entwickelten ihre Technologien weiter und vernetzten sie mit ARPANET.

Das erste Software-Unternehmen hieß System Development Corporation (SDC). Es war 1955 von RAND gegründet worden und arbeitete für ARPA. ARPA wurde später umbenannt in DARPA (D = Defense). Für die

Datenübermittlung wurde ARPANET gegründet. In den 1980er Jahren wurde SDC kommerzialisiert. Das Internet entwickelte sich aus dem ARPANET heraus.

Freigabe für zivile und kommerzielle Zwecke

DARPA wird bis heute vom Pentagon geführt und sucht mit dem Geheimdienst NSA die freie Hacker-Szene ständig nach Mitarbeitern ab. ARPANET wurde mit dem Zusammenbruch des Sozialismus offiziell beendet – der Feind war tot. Aber das Kommunikationssystem namens Internet, das zwischen den Unternehmen und den Universitäten weiterbestand, wurde 1990 für die private kommerzielle Nutzung freigegeben.

Diese Möglichkeit ergriffen zunächst US-Konzerne und dann auch europäische Konzerne etwa der privatisierten Telekommunikation, die weltweit expandierten und in die Mobiltelefonie investierten. Das erforderte mehr Computer, mehr Speicher, mehr Software, mehr internationale Unterseekabel, mehr Leitungs-Infrastruktur. Mehr als 50.000 kleine und große Unternehmen fanden dabei ihre spezialisierten Geschäftsfelder.

Tausende universitäre ARPANET-Wissenschaftler gründeten private Unternehmen und Beratungsfirmen. Diese Wissenschaftler strömten in die Wall Street-Banken und computerisierten den Wertpapierhandel über das Internet. So entwickelte David Shaw eins der ersten e-mail-Systeme, Juno, das im Internet benutzt wurde. Shaw gründete den Hedgefonds D.E.Shaw, zu dem Jeff Bezos stieß, der später Amazon gründete. Auch der Google-Gründer Eric Schmidt kommt von D.E. Shaw.

US-Regierung überwacht das Internet

1998 gründete die US-Regierung unter Präsident Clinton die Internet Corporation for Assigned Names and Numbers (ICANN). Diese zivile, non profit-Organisation sollte das schnell wachsende System koordinieren, die Nutzungsregeln festlegen und zum Beispiel die IP-Adressen vergeben (oder löschen). Die Aufsicht blieb beim Department of Commerce, der Vertrag lief zunächst bis 2009.

Frühzeitig forderten die Volksrepublik China, Russland und weitere Staaten, das Internet der UNO zu unterstellen! Die EU versuchte einen Kompromiss: Das Internet einem internationalen Rat ausgewählter Regierungen unterstellen! Doch die US-Regierungen lehnten alle Vorschläge ab. Nach dem Terror-Anschlag vom 11.9.2001 in New York beendete die US-Regierung die Diskussion und beseitigte die bisherigen Mitspracherechte der Nutzervertreter bei ICANN.

Die UNO unter Generalsekretär Kofi Annan machte 2005 einen neuen Anlauf. ICANN sollte durch WICANN ersetzt werden: World Internet Cooperation for Assigned Names and Numbers. WICANN sollte Teil der UNO-Organisation International Telecommunications Union (ITU) werden.

Doch die USA wollten aus Gründen der „Nationalen Sicherheit“ die Kontrolle auch über das Root Server-System behalten. Mit Großbritannien, Kanada und Australien – diese Staaten hatten mit dem Anhängsel Neuseeland im 2. Weltkrieg das Geheimdienstbündnis „Fife Eyes“ geschlossen – verhinderten die USA in der UNO die Internationalisierung des Internet.

Obamas „offenes Internet“

Dann versprach Obama im Wahlkampf 2008 ein „offenes Internet“. Aber seine Regierung verlängerte den 2009 auslaufenden Vertrag über die ICANN-Aufsicht bis 2016. Wegen der von Edward Snowden veröffentlichten Dokumente der US-Geheimdienste hat die US-Regierung darauf verzichtet, die formelle Aufsicht zu verlängern: Man wollte nicht den Eindruck verstärken, die USA würden das Internet weiter überwachen.

ICANN zahlte an die ehemaligen US-Außenministerinnen Condoleezza Rice und Madeleine Albright einige Millionen Dollar, damit die sich bei der US-Regierung für einen günstigen Übergang in die „Unabhängigkeit“ einsetzten. ICANN-Präsident ist nun der US-ägyptische Investmentbanker Cherine Chalaby, der die längste Zeit seiner Berufskarriere beim US-Regierungsberater Accenture verbracht hat. Vizepräsident ist Chris Disspain von der Unternehmensberatung WGP; er war Berater der Regierung von Australien, als diese zusammen mit der US-Regierung in der UNO die WICANN-Lösung ablehnte. ICANN hat weiter seinen Standort in Los Angeles und unterliegt seit 2001 dem Patriot Act.

ICANN von der US-Regierung befreit

Die Internet Corporation for Assigned Names and Numbers (ICANN) hat eine neue Vereinbarung mit dem US-Handelsministerium erzielt, die der Nonprofit-Organisation größere Unabhängigkeit gewährt und gleichzeitig mehr Länder über die Organisation informiert.

Die neue Vereinbarung, genannt Verpflichtungserklärungen, erstellt alle drei Jahre Bewertungen der ICANN-Performance, mit Mitgliedern der ICANN-Beratungsgremien, dem Department of Commerce (DOC), unabhängigen Experten und anderen, die den Review-Teams angehören.

Der DOC wird weiterhin an der Governmental Advisory der ICANN beteiligt sein. Das neue Abkommen ist ein „großer Moment, nicht nur für ICANN, sondern für das Internet“, sagte Paul Levins, Vizepräsident bei ICANN. „Diese wirklich lebenswichtige Ressource wurde von einer Regierung überwacht.“

Die US-Regierung wird „einen Platz am Tisch“ für die dreijährigen Überprüfungen haben, sagte ICANN-CEO Rod Beckstrom in einem Video auf der Website der Organisation. „Was es wirklich bedeutet, dass wir global werden“, sagte er.

„Alle Überprüfungen und alle geleisteten Arbeiten werden der Öffentlichkeit zur öffentlichen Stellungnahme vorgelegt. Aber es gibt keine separate oder einzigartige oder separate Berichterstattung an die Regierung der Vereinigten Staaten. Die gesamte Berichterstattung ist für die Welt; das ist die wirkliche Veränderung.“

Der Kapital-Digital-Militär-Komplex

Bekanntlich warnte Eisenhower bei seiner Abschiedsrede am 17.1.1961 im Oval Office vor dem „katastrophalen Aufstieg der unangebrachten Macht des militärisch-industriellen Komplexes“, zu dem er auch die Geheimdienste CIA und NSA und deren zahlreiche Tochterfirmen rechnete. Die USA führten damals mit neuer Wucht jahrelang den Kolonialkrieg Frankreichs in Vietnam fort – auch mithilfe von fake news – und bombardierten in einem „Geheimkrieg“ gleichzeitig noch Laos und Kambodscha.

Dabei spielten die Produkte und Techniken des Silicon Valley eine wichtige Rolle. Keine US-Regierung hat diese Beziehung zu verändern versucht. Mit den neuen Finanzakteuren wird der Komplex fortgeführt und erweitert.

Steve Jobs (Apple), William Gates (Microsoft) und Jeff Bezos (Amazon) überführten in aller Selbstverständlichkeit die im ARPANET entwickelten Technologien auf den zivilen Bereich. So basiert etwa auch Googles erfolgreiches Kartenprogramm Google Earth und Google Maps mit Street View auf der Software Earth Viewer: Sie war entwickelt worden, nachdem die Venture Capitalist-Firma der CIA, In-Q-Tel, 2001 den Silicon Valley-start up Keyhole aufgekauft hatte.

Earth Viewer wurde für die Überland-Spionage im Irakkrieg eingesetzt, um aus großer Höhe Einzelheiten und feindliche Bewegungen auf dem Boden zu erkennen. Die CIA hatte nichts dagegen, dass Google das Programm 2004 aufkaufte und zu Google Earth weiterentwickelte.

Suchmaschine für algorithmische Kriegsführung

Das US-Verteidigungsministerium verpflichtete Google 2017 im „Project Maven“, die Erkennungs-Software TensorFlow für Kriegsbedingungen weiterzuentwickeln. TensorFlow gehört zum Google-Bereich der Künstlichen Intelligenz (KI). Für das Pentagon-Team „Algorithmische Kriegsführung“ stellt Google über seine Tochterfirma ECS Federal mit Sitz in Northern Virginia nicht nur seine spezialisierten Ingenieure, sondern auch seinen riesigen Suchmaschinen-Datensatz zur Verfügung. Das Ministerium zahlt dafür im ersten Jahr 70 Millionen Dollar.

Mit der angepassten Software sollen die autonomen Kampfdrohnen der Zukunft außerrechtlich definierte Feinde rund um den Globus besser als bisher auslöschen. Das Projekt sollte unbedingt geheim bleiben: „Vermeidet jegliche Erwähnung, um jeden Preis“, hieß es in einer internen Google-Rundmail. Als aber 3.100 Beschäftigte

von Google in einem offenen Brief an Chef Pinchai den Ausstieg forderten, ließ er es im Silicon Valley-Sprech umdeuten: Das Projekt solle helfen, „Leben zu retten“

Weltweit integrierte Militär-Cloud

Jedi heißt ein weiteres Projekt des Pentagon: Joint Enterprise Defense Infrastructure. Es wurde Ende 2017 öffentlich ausgeschrieben. Das Militär will eine geheime Cloud-Struktur zur Vernetzung aller militärischen Formationen und Aktivitäten mit den weltweiten Militärstützpunkten und ihrer Logistik und mit den Geheimdiensten sowie zivilen Einrichtungen wie der Küstenwache aufbauen. Die GAMFAs (Abkürzung für die Digital-Konzerne Google Apple Microsoft Facebook Amazon) haben ihre Bewerbung ebenso eingereicht wie IBM und Oracle. Der Aufbau soll 10 Jahre laufen, das Budget wird mit 10 Mrd. Dollar angegeben .

Amazon entwickelt bereits mit seinen Web Services AWS für 600 Millionen Dollar einen Cloud-Dienst für die US-Geheimdienste, wie die Washington Post, die Zeitung des Amazon-Chefs Bezos, selbst bekanntgab. 2016 verkaufte Microsoft vier Millionen Lizenzen von Windows 10 an Obamas Verteidigungsminister Carter.

Microsoft macht das auch in der EU: Mit dem französischen Rüstungskonzern Thales, in Absprache mit der Macron-Regierung, entwickelt Microsoft ein Cloud-System für die Streitkräfte, das „für die Kommandozentralen wie für das Gefechtsfeld“ geeignet sei. Dagegen haben US-Geheimdienste nichts einzuwenden .

Die Wagniskapital-Tochter des Pentagon DIUx mit Sitz in Mountain View/Silicon Valley hat in ARPA-Tradition die Aufgabe, neue start ups zu fördern. „Wir sind eine schnell agierende Regierungseinheit, die Unternehmen unverdünntes (non-dilutive) Kapital zur Verfügung stellt, um Probleme der nationalen Sicherheit zu lösen“, lautet die Selbstdarstellung.

Allein der Geheimdienst CIA betreibt 137 Projekte der KI, für die er mit mehreren Silicon Valley-Unternehmen kooperiert. Dazu gehört die Abschöpfung und Auswertung von Datenmassen aus den „sozialen Medien“.