NSA

Imperiale Visionen

Das Internet ist zum Schlachtfeld zwischen den USA und China geworden. Geheimdienste und Militär bekämpfen sich, das Ziel ist die Vorherrschaft im Netz. Die NSA attackiert die Staatsführung in Peking und Konzerne wie Huawei.

Der dritte Sekretär der chinesischen Botschaft in Canberra hatte wahrscheinlich einfach Pech, als seine Mail-Adresse im Netz mehrerer westlicher Geheimdienste hängenblieb. Für die britischen Spione des GCHQ wurde der Zugang zum Postfach des Diplomaten zum Einfallstor einer Geheimoperation, die tief in die chinesischen Regierungsorganisationen führen sollte.

Über den Mail-Account des Chinesen, der in der Wirtschaftsabteilung der Botschaft arbeitete, starteten die Briten einen Angriff auf das Computernetzwerk des Handelsministeriums der Volksrepublik. Gemeinsam mit der NSA gelang es so, einen genauen Überblick über Geschäftskontakte und das Computernetzwerk des Ministeriums zu erhalten.

Das Loch habe einen „full take“, einen kompletten Mitschnitt der Kommunikation chinesischer Ministerialer, ermöglicht, schwärmen die Agenten in ihrem Bericht über eine Besprechung der Nachrichtendienste Australiens, Großbritanniens, Kanadas, Neuseelands und der USA zum Thema China. Demnach stand das chinesische Handelsministerium mindestens seit 2009 auf der Zielliste der westlichen Dienste.

Dieser Zugang ermöglichte laut dem Geheimbericht, der aus dem Archiv des ehemaligen NSA-Mitarbeiters Edward Snowden stammt, auch Einblicke in andere Regierungsorganisationen – darunter das Außenministerium, die Nachrichtenagentur Xinhua, die Export-Import-Bank, der Zoll und die Tourismusverwaltung.

Die Operationen gegen die chinesischen Regierungsbehörden, die in einem neuen SPIEGEL-Buch beschrieben werden, sind Teil einer Angriffswelle, mit der die NSA im Auftrag des Weißen Hauses systematisch Ziele in der Volksrepublik attackiert*. Washington betreibt eine digitale Offensive gegen den rasant wachsenden Einfluss der Chinesen, die als die größte Bedrohung für Amerikas globale Vormachtstellung gelten.

Diese Rolle der ultimativen Gegenmacht, die jahrzehntelang der Sowjetunion vorbehalten war, ist inzwischen China zugefallen. In der auch in Fernost beliebten US-Polit-Serie „House of Cards“ wird Peking prominent als Washingtons Nemesis gezeichnet. Die Volksrepublik hat ihren Wirkungskreis in den vergangenen 20 Jahren zu weit ausgedehnt, um sich mit der unipolaren, von den USA dominierten Weltordnung abzufinden, die nach dem Zusammenbruch des Sozialismus entstand. Pekings erklärtes Ziel ist es, zumindest die US-amerikanische Vorherrschaft im Pazifik zu brechen.

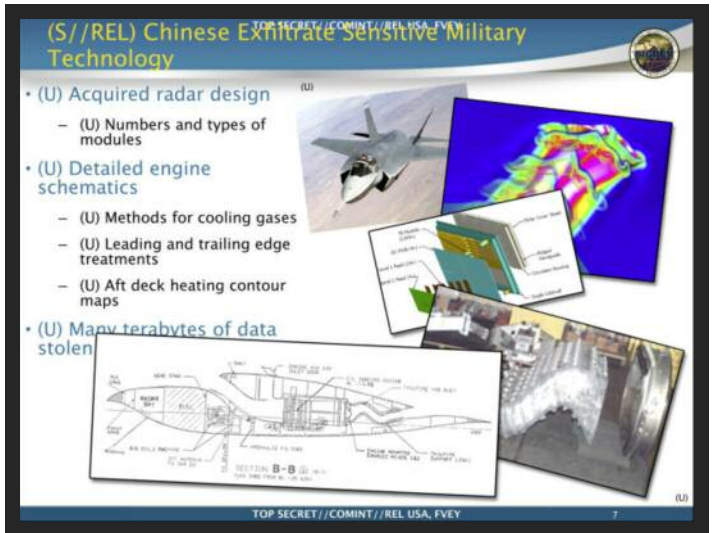
China, soll der langjährige Verteidigungsminister Robert Gates intern geklagt haben, sei „die Sowjetunion unserer Tage“. Jahrelang hätten es sich die Vereinigten Staaten erlauben können, chinesisches Foulspiel zu ignorieren, sagte US-Präsident Barack Obama nach seinem Amtsantritt. Aber seitdem die Chinesen wirtschaftlich zum Westen aufgeschlossen hätten, müsse Amerika „einen Weg finden, sie zurückzudrängen und selbst die Ellbogen auszufahren“.

Und so wird im Cyberspace ein neuer Kalter Krieg der beiden mächtigsten Nationen der Welt ausgetragen, bei dem es um Hegemonie und den geopolitischen Einfluss von morgen geht.

Die Motive sind im Fall Amerikas eher machtpolitisch, im Fall Chinas auch ökonomisch, aber beide Staaten eint ein Gedanke: Sie streben die Vorherrschaft über das Internet an, das die Regierungen in Washington und Peking als die entscheidende Veränderung des 21. Jahrhunderts ansehen. Die Armeeführungen und Geheimdienstchefs in Washington und Peking haben das Netz als das Schlachtfeld künftiger Kämpfe ausgemacht.

„Eine Informationsrevolution fegt durch die Welt, die so radikale Veränderungen erzwingt wie einst die Entwicklung der Atombombe“, schrieb der damalige NSA-Chef General Kenneth Minihan bereits im Juni 1996 in einer geheimen Mitteilung an seine Mitarbeiter. „So wie die Kontrolle der industriellen Technologie einst der Schlüssel zu militärischer und ökonomischer Macht während der vergangenen zwei Jahrhunderte war, wird die Kontrolle der Informationstechnologie der Schlüssel zur Macht im 21. Jahrhundert.“ Sämtliche Bemühungen müssten „einem einzigen Ziel“ dienen: „der informationellen Vorherrschaft für Amerika“.

Die NSA, zu der auch das Cyberkommando der Streitkräfte gehört, ist die Speerspitze dieser imperialen Vision – doch die Direktiven der chinesischen Führung klingen kaum anders. Sie sind in den Jahresplänen der Kommunistischen Partei niedergeschrieben und weichen weder im Tonfall noch in der Zielvorgabe von den Maximen aus Washington ab.



CHINESISCHE HACKER attackierten in mehreren Angriffswellen das Pentagon und amerikanische Rüstungsunternehmen und erbeuteten unter anderem Informationen über Kampfflugzeuge der USA.

* Marcel Rosenbach, Holger Stark: „Der NSA-Komplex: Edward Snowden und der Weg in die totale Überwachung“. DVA/SPIEGEL-Buchverlag, München; 384 Seiten; 19,99 Euro.

PETE SOUZA / POLARIS / STUDIO X

Präsidenten Xi, Obama in Kalifornien 2013: *Ein virtueller Feldzug beider Seiten*

„Im Informationszeitalter ist der Einfluss einer Atombombe womöglich weniger gewichtig als der Einfluss eines Hackers“, schrieben die beiden chinesischen Luftwaffen-Obristen Qiao Liang und Wang Xiangsui 1999, nur kurz nach NSA-Chef Minihan. Ausführlich setzen sich die beiden Soldaten mit Amerikas militärischen Fähigkeiten auseinander – und kommen zu dem Schluss, dass die USA nur im Cyberspace verletzlich seien.

Das Kräftemessen wird mit Bits und Bytes statt mit Raketen und Panzern ausgefochten, beide Staaten bedienen sich Schad-Software statt menschlicher Spione. Nicht einmal die Falken in Chinas Generalstab denken daran, die USA offen militärisch herauszufordern; Amerikas Überlegenheit ist in allen Waffengattungen erdrückend. Aber in den Weiten des Internets, in denen digitale Provokationen fast nie juristisch aufzuklären sind, bleibt stets die Möglichkeit der „plausible deniability“, der glaubhaften Abstreitbarkeit, Urheber zu sein. Zugleich lassen sich über das Netz Spionageangriffe auf Ministerien und Unternehmen durchführen, die früher undenkbar gewesen wären.

Bislang ist dieser virtuelle Feldzug, an dem auf beiden Seiten neben den Geheimdiensten auch die Armee beteiligt ist, nicht außer Kontrolle geraten, noch geht es nicht um Zerstörung gegnerischer Infrastruktur. Aber es ist fraglich, ob dies so bleiben wird.

„Auf dem Feld der Datensicherheit wird am Ende nur ein Gleichgewicht der Abschreckung den Frieden bewahren“, sagt der Chinese Mei Xinyu vom Handelsministerium in Peking.

Angriff aus Fernost: „Byzantine Hades“

Die Zeichnung des Flugzeugflügels, die die Angreifer kopierten, gab präzise die Konstruktion des amerikanischen Kampfflugzeugs wieder, sie zeigte, wo die Radareinheit eingebaut war, wo das Kühlungssystem und wo der Motor. Die digitalen Skizzen der US-Rüstungsfirmen betrafen die amerikanischen Tarnkappenbomber B-2 sowie technische Details über F-35- und F-22-Kampfflugzeuge und moderne Lasertechnik.

Vom Pazifik-Kommando der US-Streitkräfte stahlen die Einbrecher die Betankungspläne der Luftwaffe, von der Navy kopierten sie das Design der Luftabwehrraketen amerikanischer Atom-U-Boote. Die Luftwaffe meldete den Diebstahl von 33 000 Personalakten von Offizieren, bei der Navy wurde in 300 000 Benutzerkonten eingedrungen. Im Pentagon sollen mehr als 500 Computer befallen gewesen sein.

Mindestens 50 Terabyte an Daten, etwa das Fünffache der Bibliothek des US-Kongresses, erbeuteten die Angreifer

VINCENT YU / AP / DPA

Whistleblower Snowden 2013: *Offenbarung der dunklen Seite amerikanischer Außenpolitik*

GETTY IMAGES

Huawei-Firmensitz in Shenzhen: *NSA-Attacken in mehreren Wellen*

einer Untersuchung der NSA von 2011 zufolge in mehreren Angriffswellen. Insgesamt sei bei den Zugriffen ein Schaden von mehr als 100 Millionen Dollar entstanden.

Die Amerikaner tauften die Angriffswelle „Byzantine Hades“, nach dem griechischen Gott der Unterwelt. Sie ist die vielleicht größte und erfolgreichste aller bisherigen Attacken gewesen, die direkt gegen die amerikanische Regierung gerichtet waren. Die Urheber kamen aus China, angeblich.

In der öffentlichen Wahrnehmung des Westens stellen die Chinesen die größte digitale Bedrohung im Internet dar. Von Shanghai, Peking oder Hongkong aus betreiben klandestine Einheiten der Volksbefreiungsarmee raffinierte Netzwerk-Operationen, dringen in die Infrastruktur der US-Regierung ein und stehlen der amerikanischen Wirtschaft und der Regierung alle Interna, deren sie habhaft werden können.

Vergangenes Jahr sorgte ein Report der amerikanischen IT-Sicherheitsfirma Mandiant für Aufsehen. Darin beschrieben Analysten die Aktivitäten einer Sektion der Volksbefreiungsarmee mit dem Namen „Einheit 61398“, die in einem zwölfgeschossigen Hochhaus im Shanghaier Stadtteil Pudong residieren soll und seit 2006 angeblich mehr als 140 westliche Unternehmen infiltriert hat. Die Angriffe liefen demnach über eigene, der „nationalen Verteidigung“ zugeordnete Leitungen

Es ist Wirtschaftsspionage auf einer Metaebene, machtpolitisch motiviert.

der staatlichen Telekommunikationsgesellschaft China Telecom. Die Eliteeinheit soll rund tausend Server in 13 Ländern betrieben haben, über die sie die Zugriffe steuere und verschleiere. Unter den Firmen, die laut Mandiant Opfer von Attacken waren, befand sich ein Unternehmen, das mehr als die Hälfte der Öl- und Gas-Pipelines in Nordamerika steuert.

„Ein Hacker in China kommt an den Quellcode einer Software-Firma in Virginia heran, ohne von seinem Schreibtisch aufstehen zu müssen“, so beschrieb US-Justizminister Eric Holder die Möglichkeiten der chinesischen Cybereinheit. Und der scheidende NSA-Chef Keith Alexander nannte Chinas Datenraub den größten „Vermögenstransfer der Geschichte“.

Den Angriffen aus Fernost liegt eine Politik der kontrollierten Offensive zugrunde, die vorwiegend vom Militär betrieben wird. Die Daten aus den Rüstungsschmieden und dem Pentagon sind Gold wert bei der Modernisierung der chinesischen Armee, die zwar mit über zwei Millionen Soldaten die größte Streitmacht der Welt ist, aber in vielen Bereichen über veraltete Waffensysteme verfügt. „Wir sind in unserer Entwicklung Jahrzehnte zurück“, sagt Xu Guangyu, Generalmajor a. D.: „Selbst Indien ist uns 60 Jahre voraus.“

Vor allem Luftwaffe und Marine baut die Staatsführung in Peking derzeit aus – mit Kampfjets der fünften Generation, mit Flugzeugträgern und nuklearen U-Booten, die atomar bestückte Interkontinentalraketen abschießen können. Zugleich haben chinesische Ingenieure sogenannte „carrier killers“ entwickelt, ballistische Anti-Schiffs-Raketen, die zum ersten Mal in der Geschichte auch die bislang unangreifbaren US-Flugzeugträger treffen könnten.

In einem Bericht der eng mit der NSA verwobenen Firma Northrop Grumman über die chinesischen Aktivitäten heißt es, die Volksbefreiungsarmee verfolge eine „Strategie der elektronischen Kriegsführung in Netzwerken“. Und wenn auch nicht in jedem Einzelfall nachgewiesen werden kann, dass hinter den Angriffen staatlich beauftragte Hacker stehen, gibt es mittlerweile kaum mehr Zweifel an der Wirksamkeit dieser Digitalstrategie.

Wie effizient die Chinesen vorgehen, zeigt auch der Fall „Legion Amber“, wie er in Washington genannt wird. Er betrifft eines der größten amerikanischen Software-Unternehmen: 2012 entdeckte die NSA, dass sich chinesische Hacker mit einem ausgeklügelten Schadprogramm Zugang zum gesamten Produktionsnetzwerk der Firma verschafft hatten. Der Zugriff von außen sei derart effektiv gewesen, heißt es, dass es den Eindringlingen möglich gewesen sei, den Code der Software zu verändern. Mindestens

seit 2008 habe der Zugang existiert – unentdeckt.

Die Methoden der Chinesen sind derart aggressiv, dass sie zu einer schweren Belastung der bilateralen Beziehungen geführt haben. Die amerikanische Regierung hat die Angriffe zu einem zentralen Thema erklärt, Cybersicherheit steht auf der Tagesordnung des „Strategischen Dialogs zu Sicherheitsfragen“ zwischen Peking und Washington ganz oben. 2011 stufte das Weiße Haus die Bedrohung herauf und ordnete China die höchste Priorität bei der Bekämpfung von Cybergefahren zu. Bei einem Treffen im November 2012 sprach Obama den chinesischen Premierminister Wen Jiabao persönlich auf das heikle Thema an. Auch beim bislang letzten informellen Gipfeltreffen mit Präsident Xi Jinping im vergangenen Juni in Kalifornien waren die Vorfälle im Internet das beherrschende Thema.

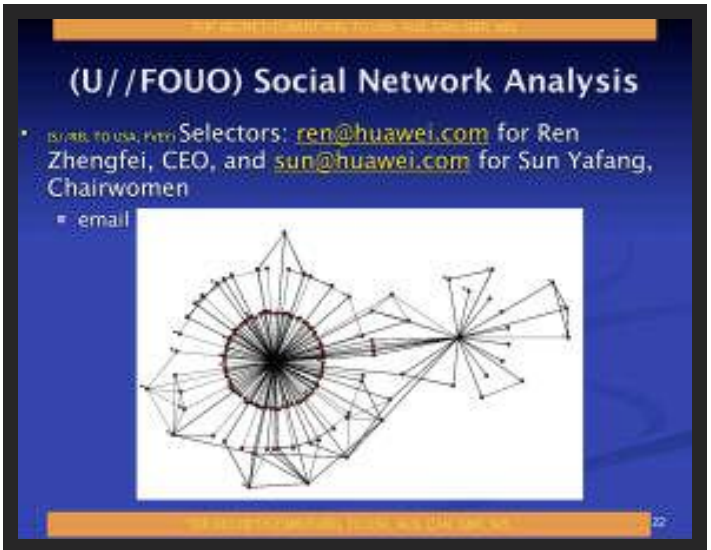
„Die internationale Gemeinschaft kann solche Aktivitäten von keinem Land akzeptieren“, warnte Obamas mittlerweile ausgeschiedener Nationaler Sicherheitsberater Tom Donilon. Cybersicherheit sei der „Schlüssel für die Zukunft“ der Beziehungen beider Länder. Was weder Donilon noch Obama einräumten, sind die eigenen Angriffskapazitäten und aktiven Spionageprogramme der USA. Auch die NSA und das Militär attackieren die chinesische Staats- und Parteiführung, sie spionieren staatliche Institutionen und Wirtschaftschefs aus und gehen gezielt gegen einzelne Unternehmen vor.

In der Begründung für das Multimilliarden-Budget der amerikanischen Dienste schreibt der Geheimdienstkoordinator James Clapper, in Bezug auf China verfolge die Regierung folgende Prioritäten: „Die Analyse und die Erfassung der wirtschaftlichen und finanziellen Führung als Ziele, das verbesserte Aufklären militärischer Stärken und das Eindringen in Computernetzwerke.“

In der von Barack Obama autorisierten Liste der Aufklärungsprioritäten vom April 2013, dem National Intelligence Priorities Framework, zählen in Bezug auf China neben der Staatsführung, der Außenpolitik und dem Militär auch Fragen der „wirtschaftlichen Stabilität und Bedrohungen des Finanzwesens“, „internationaler Handel“ sowie „aufstrebende und zerstörerische Technologien“ zu den Top-Prioritäten, die mit einer „1“ gekennzeichnet sind. Von den 31 Kategorien, mit denen die US-Regierung ihr Interesse beschreibt, ist China in 18 Fällen mit der höchsten Interessensstufe markiert. Die digitalen Schläge der Amerikaner sind, das belegen die vom SPIEGEL und der „New York Times“ ausgewerteten internen Dokumente, vielleicht weniger zahlreich als die der Chinesen, aber kaum weniger gravierend. Die NSA hingegen betont in einer Stellungnahme: „Wir setzen unsere Fähigkeiten nicht dafür ein, Betriebsgeheimnisse bei ausländischen Unternehmen zu stehlen und sie US-Firmen zur Verfügung zu stellen, um deren Wettbewerbsfähigkeit zu steigern.“

Angriff aus Amerika: Operation „Shotgiant“

Als Hu Jintao, der damalige chinesische Staatspräsident, am 18. Januar 2011 auf der Andrews Airbase im Südosten Washingtons zum Staatsbesuch eintraf, war alles vorbereitet. Der rote Teppich war ausgerollt, der amerikanische Vizepräsident Joe Biden und seine Frau Jill begrüßten den Gast aus Peking. Und auch die NSA wartete auf ihren Einsatz. Insgesamt 219 Handys von chinesischen Delegationsmitgliedern hatten die Analysten auf einer Liste notiert, die während Hus Aufenthalt abgehört werden sollten. Weitere 53 Nummern waren für funklose Überwachung vorgesehen. Der Lauschangriff verschaffte den Amerikanern wertvolle Informationen über die internen Gespräche der Chinesen.



HACKER DER NSA drangen in das Huawei-Firmennetz ein, erlangten Zugang zu den Mail-Accounts des Firmenchefs Ren Zhengfei und der Verwaltungsratschefin Sun Yafang und kopierten Quellcodes.

Wie groß das gegenseitige Misstrauen ist, zeigt das Verhalten der Chinesen bei Xi Jinpings Besuch im vergangenen Juni. Während Obama auf der kalifornischen Sunnylands-Ranch übernachtete, zog es Xi vor, im benachbarten Hyatt-Hotel abzusteigen, aus Angst vor Wanzen. Die Lauscherei bei Staatsbesuchen wird zwischen diesen beiden Ländern betrieben wie von kaum einer anderen Nation.

Wesentlich heikler ist eine andere Operation der NSA, die die Führung der Kommunistischen Partei zum Ziel hatte und für die die NSA eigens ein Team nach Peking schleuste, um nach Angriffspunkten zu suchen. Der Ausflug blieb unentdeckt.

Auf der Liste der amerikanischen Angriffsziele stehen auch zwei Telekommunikationsanbieter in China, die lange Zeit als unknackbar galten. Als es der NSA schließlich gelang, in die Computernetzwerke einzudringen, war der Jubel groß. Die abgefangene Kommunikation habe unter anderem das chinesische Militär betroffen, dank der Cyberattacke auf die Telekommunikationsunternehmen öffnete sich erstmals ein virtueller Zugang für die Amerikaner. Der Einbruch in die Kommunikation der Volksbefreiungsarmee weist einige Parallelen zum chinesischen Angriff auf das Pentagon auf.

Auch mehrere chinesische Universitäten in Hongkong und der Volksrepublik hat die NSA gehackt, wie Edward Snowden kurz nach seiner Flucht der „South China Morning Post“ verriet.

Wer dem Weißen Haus und der NSA bei ihren öffentlichen Erklärungen zur NSA-Affäre zuhört, muss genau auf die Wortwahl achten. Wir betreiben keine Industriespionage, lautet einer der Schlüsselsätze der Amerikaner, wenn es um die angebliche Ausforschung der Wirtschaft anderer Länder geht. „Es gibt zwei Unterschiede zwischen uns und den Chinesen“, sagt der ehemalige NSA-Chef Michael Hayden im SPIEGEL-Gespräch: „Wir sind besser – und wir haben Grenzen. Wir betreiben keine Wirtschaftsspionage.“ (Siehe Seite 92) Ähnlich hat es Obama in seiner Grundsatzrede im Januar 2014 versichert: „Wir sammeln keine Informationen, um amerikanischen Firmen oder der amerikanischen Wirtschaft einen Wettbewerbsvorteil zu verschaffen.“

Aber die NSA forscht Unternehmen aus, wenn sie der Meinung ist, dort entwickelten sich Techniken, die den USA als Wirtschaftsmacht gefährlich werden könnten – mit einem einzigen Unterschied: Die US-Geheimdienste geben das entwendete ausländische Know-how nicht an amerikanische Unternehmen weiter. Es ist Wirtschaftsspionage auf einer Metaebene, machtpolitisch motiviert. Das beste Beispiel dafür ist Huawei.

Der Aufstieg des 1987 in Shenzhen in der Provinz Guangdong gegründeten Telekommunikationskonzerns ist eine der schillerndsten Geschichten des chinesi-

schen Wirtschaftswunders. Die Regierung der Volksrepublik hatte das an Hongkong grenzende Shenzhen 1980 zur Sonderwirtschaftszone erklärt, woraufhin aus dem 30 000-Einwohner-Ort ein Moloch mit mehr als zehn Millionen Bewohnern entstand. Dort hat Huawei einen 21-stöckigen Glaspalast bezogen, mit eleganten Konferenzräumen, edlen Espressobars und subtropischen Zimmerpflanzen. Auf dem Firmengelände, wo etwa 40 000 Angestellte arbeiten, gibt es Palmen und Restaurants, ein Hauch von Silicon Valley liegt über dem Campus.

Mit rund 150 000 Mitarbeitern und einem Jahresumsatz von mehr als 28 Milliarden Euro ist Huawei zum zweitgrößten Netzwerkausstatter der Welt und scharfen Konkurrenten der US-Firma Cisco aufgestiegen. Der Konzern stellt Smartphones und Tablets her, aber auch Mobilfunkinfrastruktur, WLAN-Router und ist im Glasfaserkabelgeschäft aktiv, jener Technologie also, die für den Kampf der NSA um die informationelle Vorherrschaft entscheidend ist.

An der Spitze des Unternehmens steht mit Ren Zhengfei jemand, der Karriere bei der Volksbefreiungsarmee gemacht hatte. 2001 expandierte Huawei nach Amerika und eröffnete eine erste Repräsentanz in Texas. Weitere Büros des chinesischen Konzerns gibt es in mehreren amerikanischen Großstädten.

Die NSA verschaffte sich an 100 Stellen Zugang zum firmeninternen Netzwerk.

Seit mindestens 2006 attackiert die NSA den expandierenden Konzern in mehreren Wellen: 2006 lancierte sie eine erste Operation, 2009 eine zweite mit dem Codenamen „Shotgiant“. Die CIA, das FBI und das Wirtschaftsministerium unterstützten die NSA bei der Operation, auch der Geheimdienstkoordinator im Weißen Haus war eingebunden. Als Grund für die Ausforschung gab die NSA an, dass „viele unserer Ziele über Huawei-Produkte kommunizieren“ und man auf dem Stand der Technik bleiben müsse. Zudem gebe es die Sorge, „dass die Volksrepublik China die weitverzweigte Infrastruktur von Huawei zu Spionagezwecken nutzen“ könne. Unklar bleibt, ob die Geheimen dafür Belege gefunden haben.

Damit folgt die NSA einer Linie, die 2009 im „National Intelligence Estimate“, einer mit dem Weißen Haus und allen Geheimdiensten abgestimmten Lagebewertung, vorgegeben worden war: „Wir gehen mit hoher Sicherheit davon aus, dass die wachsende Rolle von internationalen Firmen und ausländischen Einzelpersonen im Bereich von Zulieferern der US-amerikanischen Informationstechnologie die Gefahr für andauernde, unsichtbare Bedrohungen erhöht.“

In einer Beschreibung der Operation gegen Huawei wird die Gefahr, die von dem Unternehmen ausgehe, als „einzigartig“ bezeichnet. Die amerikanischen Dienste seien „nicht darauf ausgerichtet, einen Fall zu behandeln, der ökonomische, geheimdienstliche und militärische Einflüsse sowie eine militärische Infrastruktur in einer Organisation vereint“. Wenn man verstehe, wie die Firma funktioniere, werde sich das in der Zukunft auszahlen.

Bislang sei die Netzstruktur westlich dominiert, doch die Chinesen arbeiteten daran, amerikanische und westliche Firmen „weniger relevant“ zu machen. Dadurch würden sich die bislang von US-Firmen dominierten technischen Standards im Internet öffnen, China könne nach und nach den Informationsfluss im Netz kontrollieren.

Nachdem die NSA Huawei in ihre Zielliste aufgenommen hatte, verschaffte sich eine Spezialeinheit laut den Geheimunterlagen an etwa 100 Stellen Zugang zum firmeninternen Netzwerk von Huawei und kopierte unter anderem eine Liste mit mehr als 1400 Kunden sowie interne Dokumente für das Training von Ingenieuren an den Huawei-Produkten. Die digitalen Einbrecher arbeiteten so effektiv, dass sie nicht nur Zugang zum E-Mail-Archiv erlangten, sondern laut einer geheimen NSA-Präsentation auch zum geheimen Quellcode einzelner Huawei-Produkte – dem Allerheiligsten der unternehmenseigenen Software.

Weil Huawei den Mail-Verkehr jedes Mitarbeiters über die Zentrale in Shenzhen leitete, wo die NSA eingedrungen war, las man in Fort Meade von Januar 2009 an einen Großteil des Mail-Verkehrs der Belegschaft mit – inklusive der Post des Firmenchefs Ren Zhengfei und der Verwaltungsratschefin Sun Yafang. Die Auswerter waren allerdings enttäuscht: Viele Mails waren Spam, Werbeangebote anderer Unternehmen, Spesenabrechnungen und Reisepläne von Ren und Sun.

„Wir haben gegenwärtig guten Zugang und so viele Daten, dass wir nicht wissen, was wir damit tun sollen“, resümierte eine Verantwortliche 2010. Ganz wohl war den NSA-Leuten offenbar nicht bei der Aktion: Da Huawei mittlerweile auch in den USA präsent sei und damit möglicherweise zumindest teilweise amerikanischem Recht unterliege, seien rechtliche Fragen zu beachten. Dennoch ist eine Firmenrepräsentanz in den USA in der Liste der Ziele aufgeführt.

Sie hätten erstmals im Sommer 2013 gehört, dass sie offenbar „ein Ziel der NSA“ seien, sagte der Vizepräsident von

MICHAEL REYNOLDS / DPA

Scheidender NSA-Direktor Alexander
Größter Vermögenstransfer der Geschichte

Huawei, John Suffolk, Ende Januar. Es sei gut möglich, dass es der NSA gelungen sei, in das Firmennetz einzudringen. Wenn die Vorwürfe stimmten, so Huawei-Sprecher Bill Plummer, „sollte mittlerweile bekannt sein, dass unsere Firma unabhängig ist und über keinerlei außergewöhnliche Beziehungen zu irgendeiner Regierung verfügt“. Eine der Abwehrmaßnahmen sei, alle Produkte einer erneuten Überprüfung zu unterziehen und die Quellcodes eigener Produkte nicht mehr an einem Ort zu speichern.

Der dauernde Druck auf das chinesische Unternehmen zeigt Wirkung. 2012 musste Huawei eine umfangreiche Untersuchung des Geheimdienstausschusses des US-Repräsentantenhauses in Washington über sich ergehen lassen. Am Ende kamen die Abgeordneten im Oktober 2012 zu dem Ergebnis, Huawei könne eine Gefahr für die nationale Sicherheit der USA darstellen. Der Firma sei nicht zu trauen.

Auch andere westliche Regierungen, darunter Australien, Großbritannien und Deutschland, begegnen dem Konzern mit Misstrauen. Nach zähen Verhandlungen machten die Briten den Chinesen eine Offerte, die diese nicht ablehnen konnten, wenn sie auf den europäischen Märkten weiter aktiv sein wollten: In Banbury in der Nähe von Oxford eröffneten sie das Cyber Security Evaluation Centre. Dort nehmen britische Experten des GCHQ Produkte von Huawei unter die Lupe und untersuchen sie auf Sicherheitslücken, eingebaute Hintertüren etwa, die chinesischen Geheimdiensten einen Fernzugriff ermöglichen könnten. Befreundeten europäischen Geheimdiensten teilten die Briten mit, auf diese Weise könnten sie möglichst viel über das Unternehmen lernen. Doch diese Vorsichtsmaßnahme scheint nicht allen Staaten zu genügen: In Australien wurde Huawei inzwischen von der Vergabe von Großaufträgen für den Netzausbau ausgeschlossen.

Snowden entlarvt die Scheinheiligkeit der Außenpolitik

Die Enthüllungen aus dem Inneren der NSA sind nicht nur für das amerikanisch-chinesische Verhältnis von besonderer Bedeutung. Sie legen auch offen, mit welcher Doppelmoral die US-Regierung auftritt. Einerseits brandmarkt das Weiße Haus die Spionageaktivitäten der Chinesen als inakzeptabel und fordert ihr Ende. Andererseits agieren die Amerikaner in China nur unwesentlich anders. Die US-Aktivitäten unterscheiden sich von den chinesischen vor allem in der Auswahl der Ziele, die weniger ökonomisch denn politisch-gesellschaftlich relevant sind. Die eigene Spionagepraxis rechtfertigen die USA stets mit den „nationalen Interessen“, einem Mantra, das beliebig ausgedehnt werden kann.

Die Einblicke in die Aktivitäten der NSA, die dank der Snowden-Unterlagen möglich sind, hätten einen ebenso simplen wie überfälligen Effekt, argumentieren die Politikprofessoren Henry Farrell und Martha Finnemore von der George Washington University: Sie würden die Scheinheiligkeit der Politik der USA ent-

larven, die ein zentrales Element der Außenpolitik Washingtons sei. Nur mit diesem Mittel könnten die Vereinigten Staaten den Rest der Welt davon überzeugen, ihnen auch dort zu folgen, wo kühle Machtpolitik an ihre Grenzen stoße. Dem hohen moralischen Anspruch Washingtons habe schon immer eine dunkle Seite gegenübergestanden.

Durch Snowdens Enthüllungen sei offenbar geworden, dass Amerika in einem ebenso großen Ausmaß hacke wie die Chinesen. Die USA könnten „diese dunkle Seite der amerikanischen Außenpolitik nicht länger abstreiten".

„Snowden hat uns das Gefühl gegeben, über Amerika zu naiv gedacht zu haben", sagt Mei Xinyu vom Pekinger Handelsministerium. „Die Sicherheitstechnologien, um unsere Daten zu schützen, stammen ursprünglich aus den USA, deshalb sind wir im Nachteil." Seit den Enthüllungen hätten er und seine Kollegen damit begonnen, auf chinesische Lenovo-Computer umzurüsten.

Wenn Obama und Xi in dieser Woche in Den Haag beim Gipfel für nukleare Sicherheit zum ersten Mal seit vergangenem Sommer zum persönlichen Gespräch zusammentreffen, wird der amerikanische Präsident höchstwahrscheinlich unangenehme Fragen beantworten müssen. Diesmal werden es die Chinesen sein, die Gesprächsbedarf haben. Die Rollen von Opfer und Täter haben sich, zumindest partiell, vertauscht. Seltsam doppelbödig klingen angesichts dieser Wahrheiten die offiziellen Verlautbarungen des Weißen Hauses zur Zukunft des Internets, wie sie Obamas Cyberberater Michael Daniel Anfang März vorgetragen hat. Die Vereinigten Staaten seien davon überzeugt, dass „wir anerkannte Verhaltensregeln zwischen Staaten im Cyberspace durchsetzen müssen", so Daniel auf einer Cyberkonferenz an der Georgetown-Universität. Obamas Berater plädierte dafür, Verhaltensregeln einzuführen, wie Regierungen ihre Cyberfähigkeiten anwenden. „Wir müssen das Risiko von ungewollten Konflikten oder Eskalationen zwischen Staaten im Cyberspace vermeiden."

Daniels Forderungen sind vernünftig, sie klingen wie notwendige Lehrsätze aus der Snowden-Debatte. Das Problem ist nur: Nicht nur die Chinesen und andere Staaten, die auf die Freiheit und Regeln im Internet wenig geben, müssten sich daran halten. Die Sätze müssten auch für die NSA und das Cyberkommando der amerikanischen Streitkräfte gelten. Ist das Weiße Haus zu diesem Schritt bereit?

Zweifel sind angebracht. Denn im Vergleich zu dem, was das Cyberkommando der US-Streitkräfte seit etwa anderthalb Jahren plant, muten die bisherigen Operationen bescheiden an. Im Oktober 2012 unterzeichnete Barack Obama eine als „streng geheim" eingestufte Direktive, die Amerika in ein neues Zeitalter überführen sollte. Darin autorisierte er die Streitkräfte, sich auf einen regulären Krieg im Internet gegen andere Nationen vorzubereiten. Ziel der Vorbereitungen sei es, heißt es in der Direktive, Computer, Informationssysteme oder Netzwerke im Ausland „zu manipulieren, zu stören, zu schwächen, zu blockieren oder zu zerstören". Ausdrücklich ist darin auch die Rede davon, dass sich die USA bei „immanenten Gefahren" das Recht auf einen Cyber-Erstschlag vorbehalten.

Mit der Anweisung beauftragte der Präsident Geheimdienstkoordinator Clapper und die Generäle, innerhalb von sechs Monaten eine Liste von „potentiellen Systemen, Prozessen und Infrastrukturen" zu erstellen, gegen die die Vereinigten Staaten offensive Cyberkapazitäten aufbauen sollten.

Willkommen bei den Vorbereitungen für den Krieg von morgen.

Marcel Rosenbach, Holger Stark, Bernhard Zand

Video: Holger Stark über die NSA-Recherchen

spiegel.de/app132014nsa
oder in der App DER SPIEGEL