

NSA

„A“ wie Angela

Der britische Geheimdienst GCHQ kundschaftet deutsche Netzfir­men aus, die NSA führte die Kanzlerin in einer Spezialdatenbank und holte 2013 die Erlaubnis ein, Deutschland zu überwachen. Leitet der Generalbundesanwalt nun Spionage-Ermittlungen ein?

Der Sitz der Firma Stellar in Hürth bei Köln ist schon von weitem erkennbar. 75 weiße Antennen prägen die Landschaft, die größten haben einen Durchmesser von 16 Metern und sind auf Stahlgerüste gestützt. Das Antennenfeld ist ein beliebter Drehort für Produktionen des nahegelegenen Fernsehsenders RTL, dessen Actionserie „Alarm für Cobra 11“ gelegentlich hier spielt.

Stellar betreibt in Hürth eine Satelliten-Bodenstation, einen sogenannten Teleport. Das Angebot richtet sich vor allem an Unternehmen und Organisationen. Unter den Kunden befinden sich Internetprovider, Telekommunikationsfirmen und Regierungen. Der Slogan des High-tech-Unternehmens lautet: „Die Welt ist unser Markt“.

Über ihre Bodenstationen und gemietete Kapazitäten von Satelliten können Firmen wie Stellar oder die Konkurrenten Cetel aus Ruppichteroth und IABG mit Sitz in Ottobrunn bei München Internet und Telefon an entlegenste Orte der Welt bringen. Sie versorgen beispielsweise Ölbohrplattformen, Diamantenminen, die Außenstellen von Großunternehmen und internationalen Organisationen.

Deshalb brauchen die Bodenstationen in Deutschland eine superschnelle Anbindung ans Internet. Sie hängen meist direkt an den wichtigsten Leitungen des Netzes, jenen mit besonders hohen Übertragungsraten, den sogenannten Internet-Backbones.

Diese Scharnierfunktion ist nicht nur für Kunden interessant, die ihre Kommunikation verbessern wollen. Sie hat die deutschen Unternehmen auch zum Ziel des britischen Nachrichtendienstes GCHQ gemacht. Geheime Unterlagen aus dem Archiv des ehemaligen NSA-Mitarbeiters Edward Snowden, die der SPIEGEL einsehen konnte, zeigen, dass die britischen Spione die Angestellten von mehreren deutschen Unternehmen überwacht und deren Firmennetze auskundschaftet haben.

Es gehe darum, „umfangreiches Wissen über zentrale Satelliten-IP-Diensteanbieter in Deutschland aufzubauen“, heißt es in einem streng geheimen, undatierten GCHQ-Papier. Ziel dieser Bemühungen

sei es, „in Deutschland vorbeifließende Internetverkehre auszukundschaften“. Drei Unternehmen sind in der Ausarbeitung namentlich genannt: Stellar, Cetel und IABG.

Die Operation, die von dem gemeinsam mit der NSA betriebenen Lauschposten im britischen Ort Bude in Cornwall koordiniert wird, gilt vor allem den Schnittstellen, an denen die Bodenstationen die Kommunikation ihrer Kunden in das allgemeine Breitband-Internet leiten.

Neben dem Ausspionieren des durchlaufenden Datenverkehrs gehe es darum, wichtige Kunden der deutschen Teleport-Anbieter zu identifizieren, ihre Ausrüster sowie künftige technische Trends aufzuklären, so die GCHQ-Leute.

Ausdrücklich werden in den Unterlagen die Mitarbeiter der Unternehmen als Ziele benannt, vor allem die Ingenieure. Im Fall von Stellar finden sich in dem GCHQ-Papier 16 Angestellte mit Namen und E-Mail-Adressen, zudem gibt es eine



GCHQ-Zentrale in Cheltenham



Abhörer Merkel in Berlin

SWNS.COM / ACTION PRESS (O); HENNING SCHACHT (U)

Liste der wichtigsten Kunden und Partner. Ihm seien bislang keine Angriffs- oder Hackversuche von Geheimdiensten bekannt gewesen, sagt Stellar-Geschäftsführer Christian Steffen. „Ich bin schockiert.“

Auch beim Wettbewerber Cetel waren die Mitarbeiter aus Bude offenbar erfolgreich. Beim Netzwerk von Cetel stießen sie nach eigenen Angaben auf vier „Server von Interesse“ und erstellten eine ausführliche Kundenliste. Laut Cetel-Chef Guido Neumann bedient sein Unternehmen hauptsächlich Kunden in Afrika und im Mittleren Osten. Die Vereinten Nationen gehören dazu und ein nord-europäisches Land, das seine diplomatischen Vertretungen über Cetel ans Netz anbinden ließ. Auch Neumann sagt, er sei überrascht.

Besonders interessant für die Geheimdienstler ist offenbar die Ottobrunner IABG, was aus einem kurzen Vermerk hervorgeht: Möglicherweise habe sich „auch schon das Netzwerkanalysezentrum der NSA“ mit dem Unternehmen beschäftigt, notierten die Briten.

Die Firma begleitet viele Großprojekte, betrieb etwa die Versuchsanlage des Transrapid und führte Tests am Airbus A380 und der „Ariane“-Rakete durch. Auch mit der Bundeswehr ist die IABG gut im Geschäft. Im Geschäftsfeld „Verteidigung und Sicherheit“ unterstütze man die Streitkräfte und ihre Beschaffungsvorhaben, heißt es in einer Eigendarstellung.

Wie Stellar und Cetel betreibt die IABG eine Satelliten-Bodenstation – die offenbar ins Visier des Nachrichtendienstes geriet. In dem britischen Dokument wird eine Liste von IABG-Routern samt deren Netzwerkadressen aufgezählt, dazu die Namen und E-Mail-Adressen von 16 Angestellten des Unternehmens als mögliche Ziele. Auf eine Anfrage des SPIEGEL antwortete die IABG nicht. Das GCHQ verweist in einer Stellungnahme darauf, man sage zu geheimdienstlichen Fragen grundsätzlich nichts.

Die Ausforschung der Unternehmen samt ihrer Mitarbeiter zählt zur Spionage – und ist damit eigentlich ein Fall für die Bundesanwaltschaft in Karlsruhe, die in der Vergangenheit in vergleichbaren Si-

tuationen gegen Russen oder Chinesen Ermittlungen eingeleitet hat.

Bislang aber tut sich Generalbundesanwalt Harald Range mit dem NSA-Komplex ausgesprochen schwer. Manch altgedienter Ermittler hat Schwierigkeiten, Amerikaner und Briten nach denselben Maßstäben zu beurteilen wie etwa die russischen Geheimdienste. Die Bundesanwälte in Karlsruhe haben einen Prüfungsvorgang angelegt; noch ist nicht entschieden, ob daraus ein offizielles Ermittlungsverfahren wird.

Zurzeit werden jene Vorwürfe geprüft, bei denen es um die Überwachung des Kanzlerinnen-Handys sowie die Ausspähung der deutschen Bevölkerung geht. Die Affäre sei „ein äußerst komplexes Thema“, sagte Range vor kurzem der „taz“: „Derzeit prüfe ich, ob überhaupt ein Anfangsverdacht für eine verfolgbare Straftat vorliegt. Nur wenn ich das bejahe, komme ich zu der Frage, ob überwiegende öffentliche Interessen einem Ermittlungsverfahren entgegenstehen – was bei Spionagedelikten zu prüfen ist.“ Eine Entscheidung soll in Kürze fallen.

Ermittlungsverfahren gegen GCHQ-Agenten oder NSA-Mitarbeiter wären ein Politikum, sie würden die ohnehin angespannten transatlantischen Beziehungen weiter belasten. Hinzu kommt, dass Range nur wenige Originalpapiere vorliegen, vor allem über die Überwachung der Kanzlerin durch die NSA.

Weitere Anhaltspunkte für die Merkel-Operation liefert nun ein Geheimdokument der NSA, in dem es um hochrangige Ziele geht. Es ist eine Präsentation des „Zentrums für Ausleitung von Inhalten“, die sich unter anderem mit der automatisierten Analyse von Daten beschäftigt. In dieser Liste sind offenbar 122 Staatschefs aufgeführt, über die die NSA im Mai 2009 Informationen sammelte. Zwölf Namen werden exemplarisch aufgelistet, darunter der von Merkel.

Die Liste beginnt bei „A“ wie Abdullah Badawi, dem gerade zurückgetretenen malaysischen Premierminister, und führt die Präsidenten von Peru, Somalia, Guatemala, Kolumbien ebenso auf wie den Weißrussen Alexander Lukaschenko. Der letzte Name auf der Liste, Nummer 122, ist Julija Timoschenko, die damals noch ukrainische Premierministerin war. Die Staatschefs sind alphabetisch geordnet nach Vornamen. Merkel ist unter „A“ an Position 9 geführt, hinter dem damaligen malischen Präsidenten Amadou Toumani Touré und vor dem syrischen Diktator Baschar al-Assad.

Aus dem Dokument geht hervor, dass Angela Merkel in der sogenannten Target Knowledge Database (TKB) geführt wurde, einer Datenbank zu Zielpersonen. Laut einer NSA-internen Definition können Analysten damit „komplette Profile“ von Individuen erstellen. In dem Dossier werben die NSA-Leute am Beispiel der

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

Machine vs. Manual Chief-of-State Citations

Nymrod (machine-extracted) Citations					Last TKB Manual Update
	Name	Role	Code	Cites	
1	Abdullah Badawi	Malaysian Prime Minister	cos	> 100	10/15/2007
2	Abdullahi Yusuf	Somali President	cos	> 300	N/A
3	Abu Mazin	(Mahmud 'Abbas) PA President	cos	> 200	5/20/2009
4	Alan Garcia	Peruvian President	cos	> 100	N/A
5	Aleksandr Lukashenko	Belarusian President	cos	> 80	N/A
6	Alvaro Colom	Guatemalan President	cos	> 200	N/A
7	Alvaro Uribe	Colombian President	cos	> 700	N/A
8	Amadou Toumani Toure	Malian President	cos	> 80	N/A
9	Angela Merkel	German Chancellor	cos	> 300	N/A
10	Bashar al-Asad	Syrian President	cos	> 800	N/A
...
122	Yuliya Tymoshenko	Ukrainian Prime Minister	cos	> 200	N/A

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

ZIELPERSON 9: Eine streng geheime Liste der NSA enthält Namen von Staatschefs, die als Zielpersonen erfasst sind. Angela Merkel wurde in einer Datenbank geführt, die Erkenntnisse aus Telefon- und Computerüberwachung sowie aus offenen Auswertungen beinhaltet. Über die Kanzlerin wurden 2009 mehr als 300 Berichte erfasst.



Whistleblower Snowden in einer Videokonferenz

Von angeleiteten Wachhunden

Zum neuen SPIEGEL-Buch über die NSA – und warum die Lehre aus der Snowden-Affäre nur eine Stärkung der deutschen Spionageabwehr sein kann *Von Hans-Georg Maaßen*

Während der Untersuchungsausschuss des Deutschen Bundestags seine Tätigkeit noch gar nicht aufnehmen konnte, sind Marcel Rosenbach und Holger Stark mit ihrer Arbeit bereits fertig. Die SPIEGEL-Journalisten, die offensichtlich Zugang zu Dokumenten von Edward Snowden haben, geben in „Der NSA-Komplex“ eine umfassende und detaillierte Darstellung der Person Edward Snowdens und der Hintergründe seines Asyls in Russland. Sie zitieren aus verschlüsselten Chats mit ihm, sie berichten von Besuchen bei der NSA, im Kanzleramt und im Weißen Haus, von Gesprächen mit aktiven und ehemaligen Nachrichtendienstlern weltweit, sogar ein früherer Stasi-Oberst kommt zu Wort. Das Buch enthält viele Informationen aus Snowdens Unterlagen, etwa über das gemeinsame Anzapfen von Glasfaserkabeln durch die NSA und das britische GCHQ. Spektakulär Neues ist ihm nicht zu entnehmen, die Leistung besteht darin, die vorliegenden Erkenntnisse zu einem Bild zusammenzufügen.

Der „NSA-Komplex“ schildert uns Snowden als den Heldentypus einer neuen Generation, die radikal moralisch denke und argumentiere. In der Tat erfährt man einige durchaus interessante Details aus dem Leben des 30-jährigen Autodidakten – ohne dass man der SPIEGEL-untypischen Verehrung anheimfallen müsste. Es ist nicht allein der zuweilen schwärmerische Duktus, der irritiert, sondern auch der Versuch, die Whistleblower als eine neue digitale, soziale Bewegung zu adeln. Snowden

wird zum Sinnbild eines Generationskonflikts stilisiert: Politik 1.0 vs. Politik 2.0, eine Begegnung zweier Welten, die nur begrenzt kompatibel seien.

Diesem Heldentypus stellen die Autoren in düsteren Farben einen weltumfassenden Überwachungsapparat von NSA und GCHQ gegenüber, dem niemand mehr enttrinnen kann. Überdeutlich wird die Antriebskraft der Autoren für das Schreiben des Buchs, ihre Angst vor einer totalen Überwachungsgesellschaft, in der die Dienste alles über die Menschen wissen und ihre Gedanken dank „big-data-Analyse“ schon vorhersehen, ehe sie gedacht worden sind. Eine Angst vor einer „schönen neuen Welt“ im Sinne von Aldous Huxley und vor einem Nordkorea 2.0.

Rosenbach und Stark beschreiben dies im Kapitel „Wir Überwachten“. Ist dies vielleicht eine typische German Angst? Ist diese Angst vor einem Überwachetsein durch die NSA nicht der NSA-Komplex im psychologischen Sinne? Warum sonst findet Snowden in nahezu keinem anderen Land der Welt so viel Aufmerksamkeit wie in Deutschland? Warum ist die NSA nicht in vergleichbarer Weise ein Thema in Frankreich, Spanien, Italien, Russland, China oder Japan? Alles Staaten und Bevölkerungen, die ebenfalls von den Snowden-Dokumenten betroffen sein müssten.

Vielleicht liegen dieser Angst zwei Missverständnisse zugrunde: zum einen das Missverständnis, dass schon durch das bloße Speichern von Daten das Verhalten von Menschen überwacht wird.

Und zum anderen die Annahme, die im vergangenen Herbst die öffentliche Diskussion leitete: Wenn die NSA noch nicht einmal davor zurückschreckt, die Kanzlerin abzuhören, dann müsse auch der einfache Bürger damit rechnen, überwacht zu werden.

Wir wissen, dass die USA und andere Staaten ein anderes Datenschutzverständnis haben als wir – dass sie das bloße Speichern von Daten datenschutzrechtlich für irrelevant halten. Aber bedeutet das Speichern schon Überwachung? Warum sollten die USA die E-Mails der Deutschen lesen und ihre Gespräche mithören? Wenn ich die Meinungsumfragen im Zusammenhang mit der letzten Bundestagswahl richtig verstanden habe, teilen die Menschen in Deutschland diese Angst nicht. Sie glauben nicht, dass sich irgendeine finstere Behörde für ihre persönlichen E-Mails und Telefongespräche interessiert. Sie fühlen sich nicht überwacht, sondern vor Terroranschlägen geschützt. Und das, wie das Buch am Beispiel der sogenannten Sauerland-Gruppe in Erinnerung ruft, auch dank Hinweisen ausländischer Partnerdienste. Ich bin der Überzeugung, dass selbst ein Nachrichtendienst wie die NSA überfordert wäre, wollte sie den gesamten Telekommunikationsverkehr der Deutschen mitlesen und mithören. Sie müsste hierfür vermutlich mehrere hunderttausend Mitarbeiter einstellen.

Das Thema der massenhaften Speicherung deutscher Daten durch ausländische Dienste und das Belauschen der Telekommunikation von politischen Ent-

scheidungsträgern in Deutschland darf allerdings nicht kleingeredet werden. Und es wäre sicherlich ein Fehler, den Blick auf NSA und GCHQ zu verengen. Es gibt Staaten, die vielleicht vergleichbare Möglichkeiten haben, die aber nicht zu unseren Freunden zählen. Davon ausgehend stellen Rosenbach und Stark Lösungsansätze vor, angefangen beim Selbstschutz der Betroffenen im Umgang mit eigenen Daten und der eigenen Telekommunikation bis zur Frage, was der Staat zu seinem Schutz und dem Schutz seiner Bürger tun kann.

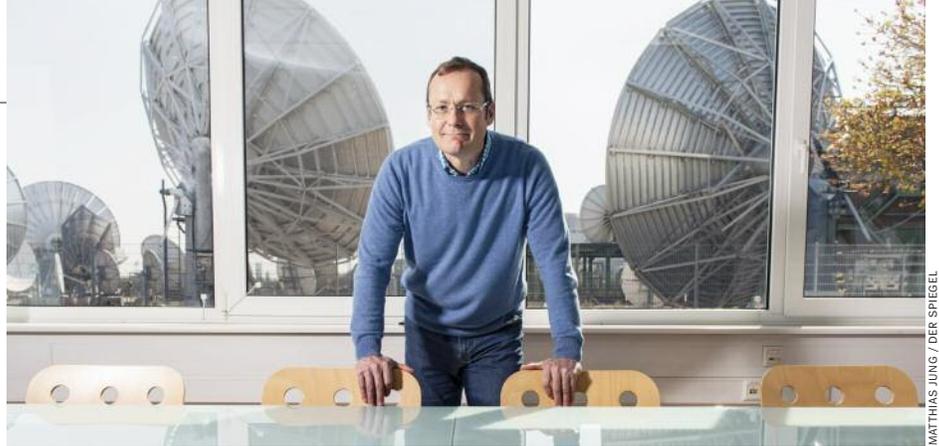
Kritik an unseren Freunden in Washington und London hilft nicht wirklich weiter: Wir müssen uns an unsere eigene Nase fassen. Wenn wir im Umgang mit unseren Daten so offen sind wie eine offene Haustür, dann dürfen wir uns nicht wundern, wenn nicht nur unsere Freunde, sondern auch andere in unserem Haus ein- und ausgehen. Es ist keine Lösung, dann auf den Dieb zu schimpfen und den Wachhund zu prügeln, vor allem wenn er angeleint war und einen Maulkorb trug. Die Antwort darauf kann nur Aufklärung und ein verbesserter Schutz sein – rechtlich, materiell, nachrichtendienstlich. Informationssicherheit ist Teil der staatlichen Souveränität und grundgesetzlich geschützter privater Integrität. Cyber-Sicherheit kann nur als vernetzte Sicherheit verstanden werden.

Die Snowden-Enthüllungen führen dazu, dass in der Öffentlichkeit der Blick einseitig auf die Aktivitäten der USA und Großbritanniens gelenkt wird, aber über vergleichbares Verhalten anderer Staaten kaum noch berichtet wird. Die Veröffentlichungen haben allerdings auch positive Aspekte, zumindest mittelbar. Mit der Diskussion wird nicht nur die Anfälligkeit der digitalen Welt für Ausspähversuche deutlich – angefangen bei der bedenkenlosen Nutzung von Smartphones bis hin zu einer elementaren Gefährdung kritischer Infrastrukturen. Sie hat das Problembewusstsein gestärkt.

Marcel Rosenbach und Holger Stark haben ein faktenreiches, wichtiges, leidenschaftlich geschriebenes Buch vorgelegt, das den Leser mitnimmt. Sie haben ihren Blick auf Snowden und die NSA. Man muss ihrer Analyse nicht folgen, aber man wird sie beachten und seine eigenen Argumente daran prüfen müssen.



Maaßen, 51, ist Präsident des Bundesamts für Verfassungsschutz und zuständig für die Abwehr von Spionage.



MATTHIAS JUNG / DER SPIEGEL

Hightech-Unternehmer Steffen: „Ich bin schockiert“

Staatschefs für die maschinelle Analyse von Informationsquellen zu den jeweiligen Zielpersonen.

Als durchsuchbare Quelle wird in dem Dokument unter anderem die Datenbank „Marina“ genannt, die abgeschöpfte Kommunikationsmetadaten aus aller Welt enthält. Die Erwähnungen in der Datenbank stammen aus Geheimdienstberichten, Transkripten von abgefangenen Faxen, aufgezeichneten Gesprächen und abgefangener Kommunikation zwischen Computern. Die Datenbank diene dazu, „über Zielpersonen Informationen zu finden, die sonst schwer aufzufinden sind“.

Die manuelle Pflege der Datenbank mit hochrangigen Zielen sei aufwendig und langsam, das System habe weniger als 200 000 Personen verwalten können. Die automatische Erfassung erleichtere

Ein Sondergericht autorisierte die NSA, Deutschland zu überwachen.

dagegen die Speicherung und habe es ermöglicht, mehr als drei Millionen Einträge zu verwalten, Namen und dazugehörige Erwähnungen.

Glaubt man der Tabelle, dann ist Merkel's Datensatz bereits auf maschinelle Verwaltung umgestellt, ein manuelles Update war jedenfalls im Mai 2009 nicht verfügbar. Das Dokument könnte ein weiteres Puzzlestück für die Ermittler in Karlsruhe sein, das belegt, dass die Kanzlerin offiziell als Spionageziel erfasst war.

Neben der Überwachung der Bundeskanzlerin beschäftigt sich die Bundesanwaltschaft mit der Frage, ob die NSA massenhaft die deutsche Bevölkerung ausspioniert hat. In den internen NSA-Materialien findet sich ein Wochenbericht der Abteilung „Special Sources Operations“ (SSO) vom März 2013, jener Ab-

teilung, die unter anderem für den Zugang der NSA zu den großen Internetdatentrassen zuständig ist, den Glasfaserkabeln.

Darin berichtet das Team, das den Kontakt zu US-Telekommunikationsanbietern wie AT&T oder Verizon pflegt, von der rechtlichen Grundlage, auf der die Daten bestimmter Länder überwacht würden. Dem SSO-Bericht zufolge autorisierte das für Anträge des Geheimdienstes zuständige Sondergericht, der sogenannte Fisa-Court, die NSA am 7. März 2013, Deutschland zu überwachen. Die Gerichtsentscheidung trägt das Aktenzeichen 13-319.

Welche Daten genau davon betroffen sind, lässt sich anhand der Dokumente nicht sagen, die NSA möchte sich dazu nicht äußern. Die amerikanische Bürgerrechtsorganisation Aclu geht davon aus, dass der Behörde damit der Zugriff auf die Kommunikation aller deutschen Staatsbürger erlaubt ist, unabhängig von der Frage, ob die Betroffenen irgendwie verdächtig sind. Das entsprechende Gesetz, der „Fisa Amendments Act“ von 2008, erlaube es der NSA, pauschal zu überwachen, ohne dem Gericht Einzelfälle vorlegen zu müssen.

Solche Ermächtigungen des Gerichts gibt es etwa für China, Mexiko, Japan, Venezuela, Jemen, Brasilien, Sudan, Guatemala, Bosnien und Russland. In der Praxis nutzt die NSA die Ermächtigungen unterschiedlich, mal zur Überwachung von Telekommunikationsunternehmen, mal gegen Einzelpersonen.

„Wir haben bislang keine Erkenntnisse, dass Internetknoten in Deutschland durch die NSA ausspioniert wurden“, sagte der Präsident des Bundesamts für Verfassungsschutz, Hans-Georg Maaßen, im Sommer 2013.

Vielleicht müssen die Amerikaner das gar nicht, jedenfalls nicht in Deutschland. Sie können sich vielmehr bei den großen US-Anbietern wie AT&T oder Verizon bedienen, über deren Infrastruktur ein großer Teil des Internetverkehrs abgewickelt wird, und dort auf die Daten aus Deutschland zugreifen. Aus amerikanischer Perspektive ganz legal.

Laura Poitras,
Marcel Rosenbach, Holger Stark

Der Artikel basiert auf dem SPIEGEL-Buch „Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung“ von Marcel Rosenbach und Holger Stark, das diese Woche in den Buchhandel kommt. Es hat 383 Seiten, ist bei DVA erschienen und kostet 19,99 Euro.