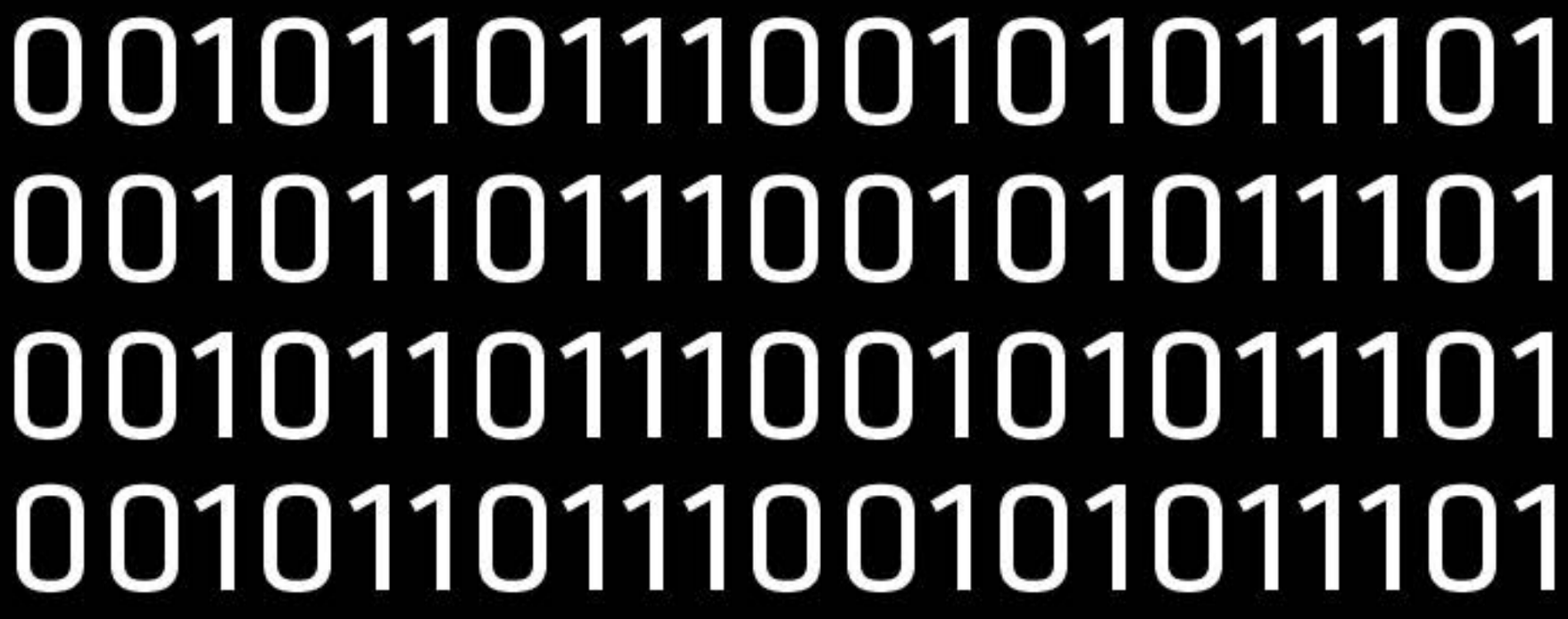
SO. DIGITAL

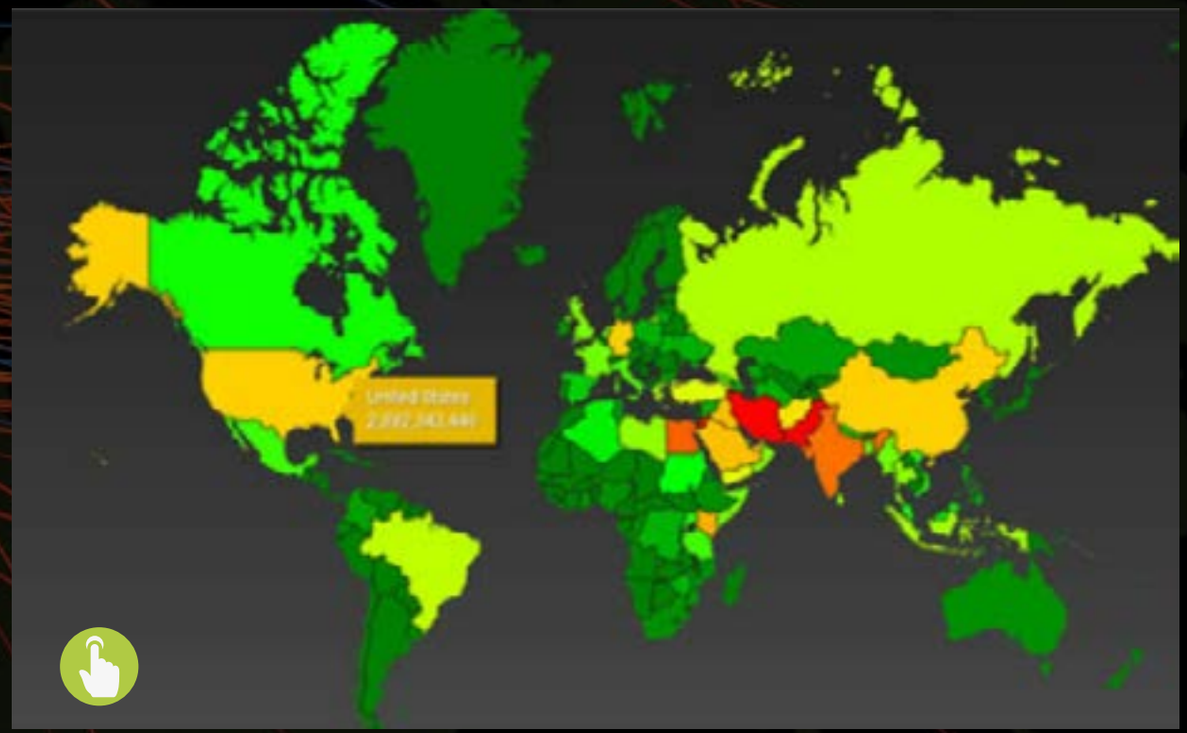


Unter Generalverdacht

Wie erfolgreich ist das Überwachungsprogramm der NSA? Der US-Geheimdienst kontrolliere vor allem unschuldige Personen, sagen Kritiker. Denn Terroristen wüssten, wie sie unbemerkt miteinander kommunizieren könnten.

VON MARKUS WERNING

Ist es wirklich so einfach, die Mitarbeiter des US-Geheimdienstes NSA zu ärgern? Mit einer E-Mail? In der vergangenen Woche rief jemand im Internet dazu auf. Millionen Menschen sollten ihren Freunden denselben Text schicken. Er nannte es die „Operation Troll the NSA“. „Sie sagen, sie würden unsere Nachrichten nicht lesen“, schrieb er. „Warum testen wir es nicht?“ Edward Snowden behauptet schließlich etwas anderes.



Die Zeitungen „Guardian“ und „Washington Post“ hatten vor einer Woche Unterlagen des ehemaligen Mitarbeiters der National Security Agency (NSA) veröffentlicht, die Karte rechts gehört dazu. Demnach fängt der US-Geheimdienst seit Jahren unter dem Namen „Prism“ massenweise E-Mails, Fotos und vieles mehr von Menschen aus aller Welt ab, speichert sie und wertet sie aus. „Mal sehen, wie sie damit umgehen“, meinte der Initiator der „Operation Troll the NSA“.

Er hatte eine E-Mail formuliert, wie sie jeden Tag von vielen Menschen geschrieben wird: Der Verfasser beklagt sich über den Chef, schwärmt von einer Fernsehserie und beschreibt seine nächste Urlaubsreise. Aber er verwendete Begriffe wie Manhatten, Marathon, Bombe, Gift und Flugschule. „Lasst uns die NSA-Scanner blockieren“, sagte er. „Das wird ein Spaß.“ Mehr als 50 000 Menschen wollten ihn unterstützen.

Es wäre erschreckend, wenn sie damit Erfolg gehabt haben sollten. Nicht nur, weil dann Snowden Recht hätte und weltweit unzählige Internetnutzer ohne konkreten Anlass von der NSA überwacht würden. Wie bei einer Rasterfahndung. Sondern auch, weil Begriffe wie Bombe und Flugschule in einer E-Mail nicht ausreichen sollten, damit ein US-Geheim-

dienst auf jemanden aufmerksam wird und derjenige als Terrorverdächtiger gilt. Etwas ausgereifter sollten die Methoden der NSA schon sein.

Wer wann mit wem?

Um große Datenbestände zu analysieren, sind mehrere Verfahren denkbar. Dazu gehört zwar auch die Suche nach Begriffen. Aber wahrscheinlich würden die gesammelten Informationen zunächst gefiltert, um die riesige Menge zu reduzieren: Allein im März 2013, sagt Snowden, soll die NSA weltweit fast 100 Milliarden Datensätze abgefangen haben. Sie stammen aus den USA, vor allem aber aus dem Iran und Pakistan, auch aus Deutschland. Ein naheliegendes Selektionskriterium wäre zum Beispiel: Wer hat wann mit wem kommuniziert? Sollte dieser Abgleich von Sender, Empfänger, Ort und Zeitpunkt auffällige Ergebnisse bringen, könnte der Inhalt der Daten untersucht werden – automatisch vom Computer, mit Hilfe von Algorithmen.

Solche Analysen werden nicht nur vom US-Geheimdienst gemacht, sondern genauso von Wissenschaftlern und Unternehmen verschiedener Branchen weltweit. Viele Firmen

sonntag Interview

... mit CHRISTOPH MEINEL, Direktor des Hasso-Plattner-Instituts für Softwaresystemtechnik (HPI), Potsdam.

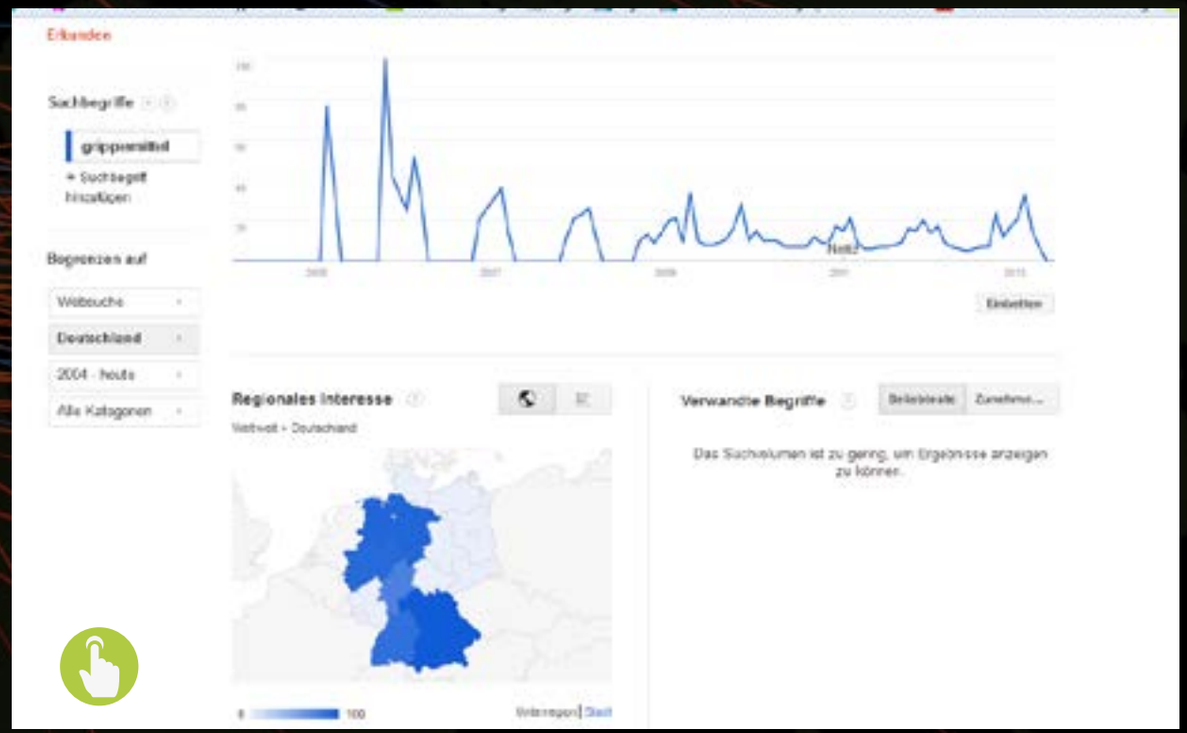
»Keiner will der Richter sein«

E-Mails, Fotos, Videos, Facebook-Postings: Im Internet fallen täglich sehr viele Daten an. Wie schnell können diese analysiert werden?
Früher hätte eine Analyse von großen Datenmengen eine Ewigkeit gedauert, heute bekommen Sie in Realzeit ein Ergebnis. Nehmen Sie zum Beispiel eine

BITTE SCROLLEN

werten zum Beispiel Informationen aus, die sie von ihren Kunden bekommen, um ihnen gezielter Werbung zu schicken. Beispiel Amazon.

Eine Datenanalyse kann aber auch sinnvolle Ergebnisse hervorbringen, das kann jeder testen: Google Trends zeigt unter anderem, wann wo nach einem Grippemittel gesucht worden ist. Dadurch lässt sich nachvollziehen, wie sich die Krankheit ausgebreitet hat. Künftige Epidemien verlaufen vielleicht genauso, die Menschen könnten sich dann darauf vorbereiten. „Wenn große Datenmengen ausgewertet werden, sind aussagekräftige Ergebnisse möglich“, sagt Peter Leppelt, Geschäftsführer der Datenschutzfirma Praemandatum aus Hannover.



Allerdings geht es um Wahrscheinlichkeiten. Die Analyse könne Ungenauigkeiten und Fehler enthalten, warnt Leppelt. Wer in diesem Jahr krank war, muss es im nächsten nicht wieder sein. Vielleicht wohnt er auch woanders. Außerdem entwickeln sich Grippeviren weiter. Oder: Wer im Internet nach Hasspredigten suche, plane nicht automatisch einen Anschlag, sondern promoviere über das Thema Terrorismus, sagt Leppelt. Aber erkennt ein Algorithmus den Unterschied? „Ich würde keine Menschenleben oder auch nur den Ruf eines Bürgers von einer Datenanalyse abhängig machen.“

Ein Problem, dass nicht nur Leppelt sieht: Die NSA ermittle sicherlich verdächtige Personen, überwache dabei wahrscheinlich aber auch viele Unschuldige, sagen Karoline Busse und Falk Garbsch vom Chaos Computer Club (CCC) in Hannover. „Würden tatsächlich nur real Verdächtige in den Fokus

geraten, so hätten wir Datenschützer ein erheblich kleineres Problem mit der Praxis von Prism“, kritisiert Thilo Weichert, Datenschutzbeauftragter des Landes Schleswig-Holstein. Aus einem Spaß wie „Troll the NSA“ kann dann schnell Ernst werden: In der Vergangenheit hätten die USA schon jemandem wegen bestimmter Äußerungen die Einreise verboten, sagt Weichert. Außerdem müsse damit gerechnet werden, dass die US-Behörden „das gesamte persönliche Verhalten im Internet umfassend und minutiös“ verfolgten. Und dann?

Datenschützer können wenig ausrichten

Der Bundesdatenschutzbeauftragte Peter Schaar sieht kaum eine Möglichkeit für Europäer, sich gegen die Überwachung zu wehren. Die Gesetze der USA schützten nur die Menschen in den Vereinigten Staaten. „Ich wüsste deshalb nicht, wie Betroffene aus Europa die Rechtmäßigkeit des Datenzugriffs durch US-Gerichte überprüfen lassen können“, sagt Schaar. „Auch europäische Datenschutzbehörden können hier wenig ausrichten.“ Er erinnert deshalb an die geplante europäische Datenschutzgrundverordnung. Die Mitgliedsstaaten der EU verhandeln gerade darüber. „Ursprünglich waren wichtige Schutzvorkehrungen vorgesehen.“ Drittstaa-

sonntag interview

... mit THILO WEICHERT, Landesbeauftragter für den Datenschutz Schleswig-Holsteins

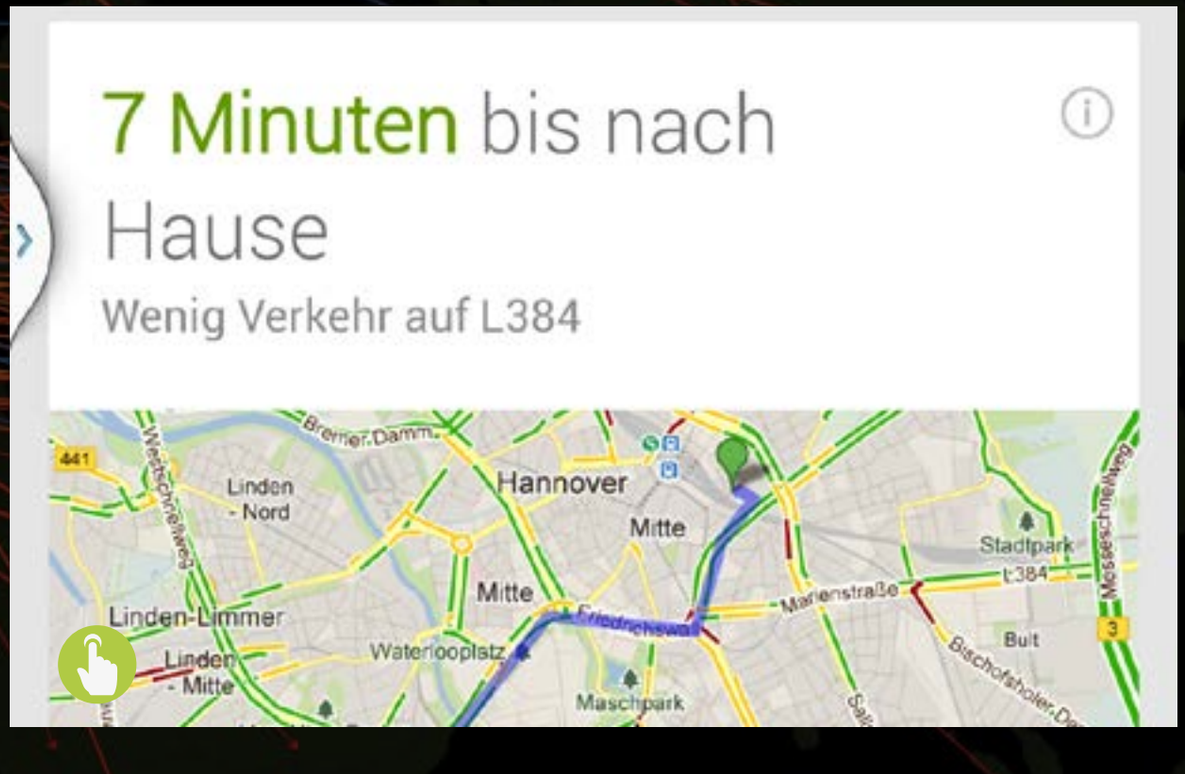
»Knapp 100 Prozent Unschuldige«

Angenommen, ich benutze Google Mail, schreibe darüber eine Nachricht und schimpfe darin auf die USA, zum Beispiel mit den Worten „Nieder mit den USA“. Muss ich damit rechnen, dass die USA auf mich aufmerksam werden?

Sicher ist, dass diese Mail in die Verfügungsmacht der

BITTE SCROLLEN

ten wie den USA sollte nur unter strengen Voraussetzungen der Zugriff auf privat gespeicherte Daten erlaubt werden. Die Passage wurde aber wieder gestrichen. „Dieser Ansatz sollte wieder aufgegriffen werden“, fordert Schaar. Spätestens aber wenn in Europa wieder ein Anschlag verübt werde, kippe auch hier die Stimmung, befürchten dagegen Busse und Garbsch vom CCC. Dann werde zum Beispiel wieder nach der Vorratsdatenspeicherung gerufen. „Mit der Begründung, dass wir wissen müssten, wer mit wem kommuniziert.“



Busse und Garbsch verzichten auf Dienste von US-Firmen wie Google, Facebook und Microsoft so gut es geht. Und zwar nicht erst seit Prism. Aber was Snowden berichtete, hat sie in ihrem Misstrauen bestätigt: Angeblich kann der US-Geheimdienst direkt auf die Server mehrerer Unternehmen zugreifen: „Die NSA hat eine Infrastruktur aufgebaut, die ihr erlaubt, fast alles abzufangen.“ Die Konzerne bestreiten das. Diese Behauptung sei falsch, versicherte Google. Facebook und Microsoft veröffentlichten Zahlen, um das zu bestätigen: Im zweiten Halbjahr 2012 hätten die US-Behörden Anfragen zu 19 000 (Facebook) und 31 000 Kunden (Microsoft) gestellt. Es sei um vermisste Kinder, gewöhnliche Kriminalfälle und Terrordrohungen gegangen. Die Behörden hätten immer nur so viel erfahren, wie es das Gesetz verlange.

Zum einen ist das aber wahrscheinlich schon mehr als in anderen Ländern. Der Patriot-Act – das Gesetz ist eine Reaktion auf die Anschläge vom 11. September – räumt den Ermittlern weitreichende Befugnisse ein. In Europa, vor allem in Deutschland seien die Hürden für eine Datenabfrage deutlich höher, versichert Oliver Dehning von Antispameurope in

Hannover. „Es muss ein richterlicher Beschluss vorliegen, und der Betroffene wird darüber informiert.“ Seine Firma filtert für Unternehmen Spam aus dem E-Mail-Verkehr. Die Daten laufen dafür über die Server der Deutschen. Jährlich gebe es vereinzelte Anfragen von Behörden, sagt Dehning.

Die USA wollen die Sorgen zerstreuen

Zum anderen hätte die NSA technisch gesehen auch andere Möglichkeiten, um E-Mail, Chats und Dokumente abzufangen, berichtet das Schweizer Fernsehen. Die Server der Unternehmen stehen in den USA, der Geheimdienst könnte über Backbones (große Hauptleitungen) oder Speicherplatz-Anbieter den Internet-Verkehr mitschneiden. Andernfalls wäre nicht erklärbar, warum Snowden zu Journalisten sagte: „Ich kann ihre E-Mails, Passwörter, Gesprächsdaten, Kreditkarteninformationen bekommen.“

In der Praxis wird es für die meisten Menschen aber schwierig werden, auf Dienste wie Google, Facebook und Microsoft zu verzichten. Die Unternehmen hätten „eine monopolartige Stellung“ erreicht, ein Verzicht sei „kein gangbarer Weg“, meint Schaar. „Wer sensible Daten in der Cloud ablegen will, sollte diese verschlüsseln“, rät er. Ein Arzt oder Anwalt, der das versäume, „macht sich eventuell sogar strafbar“. Praemandatum-Chef Leppelt empfiehlt eine Anbieterstreuung: „Ich möchte mein Leben nicht einem einzelnen Unternehmen anvertrauen.“

Die USA bemühen sich dagegen, die Sorgen der Deutschen zu zerstreuen. Barack Obama wolle Kanzlerin Angela Merkel (CDU) bei seinem Besuch am Dienstag erklären, dass das US-Spähprogramm allein zur Vereitlung von Terroranschlägen diene und im Interesse beider Länder sei, sagte der stellvertretende Nationale Sicherheitsberater Ben Rhodes. Vorher hatte das Weiße Haus sich dazu gezwungen gesehen, auf Erfolge durch Prism zu verweisen. 2009 seien zwei Bombenattentate vereitelt worden. Der Anschlag auf den Marathon in Boston allerdings nicht. Fraglich ist sowieso, ob Terroristen nicht damit rechnen, dass E-Mails über Dienste wie Google abgefangen werden. „Die gefährlichen Personen wissen, wie sie davon kommen“, sagt Leppelt. Die meisten Privatleute dagegen nicht. Weichert rechnet damit, dass „zu knapp 100 Prozent Unschuldige überwacht werden“. Die NSA hat bisher nichts über ihre Trefferquote verraten.