



Das kann doch nicht so einfach sein

Doch, sagen Informatiker, es ist durchaus möglich, dass jemand in Frankfurt nahezu den gesamten Internetverkehr mitschneidet – und es fällt niemandem auf. Eine Anleitung.

VON MARKUS WERNING



Frankfurt wäre ideal. Wollte jemand wissen, was sich die Menschen in Deutschland über das Internet schicken, gäbe es keinen besseren Ort, um E-Mails, Fotos und Dokumente abzufangen. Denn hier ist einer der wichtigsten Knotenpunkte des World Wide Web. Egal, ob Sie etwas über Google suchen oder Facebook aufrufen: Die Daten laufen fast immer hierüber. Es gibt Karten, die das sehr gut illustrieren. Tippen Sie doch einmal auf „Warum ausgerechnet Frankfurt?“. Deshalb sind Fachleute überhaupt nicht über Berichte erstaunt, wonach der US-Geheimdienst NSA den Datenverkehr an Internet-Knotenpunkten in Süd- und Westdeutschland mitschneide – und vor allem in Frankfurt. Das Bundesinnenministerium hat dafür zwar nach eigenen Angaben keine Belege. Aber je nachdem, für welche Variante sich ein Geheimdienst entscheiden würde, wäre es gar nicht zu bemerken, erklären die Experten. Machbar sei es auf jeden Fall: „Das kann jeder, der das technische Grundwissen dafür hat und sich die technischen Geräte besorgt“, meint Marko Schuba, Professor für Elektrotechnik und Informationstechnik an der Fachhochschule Aachen.



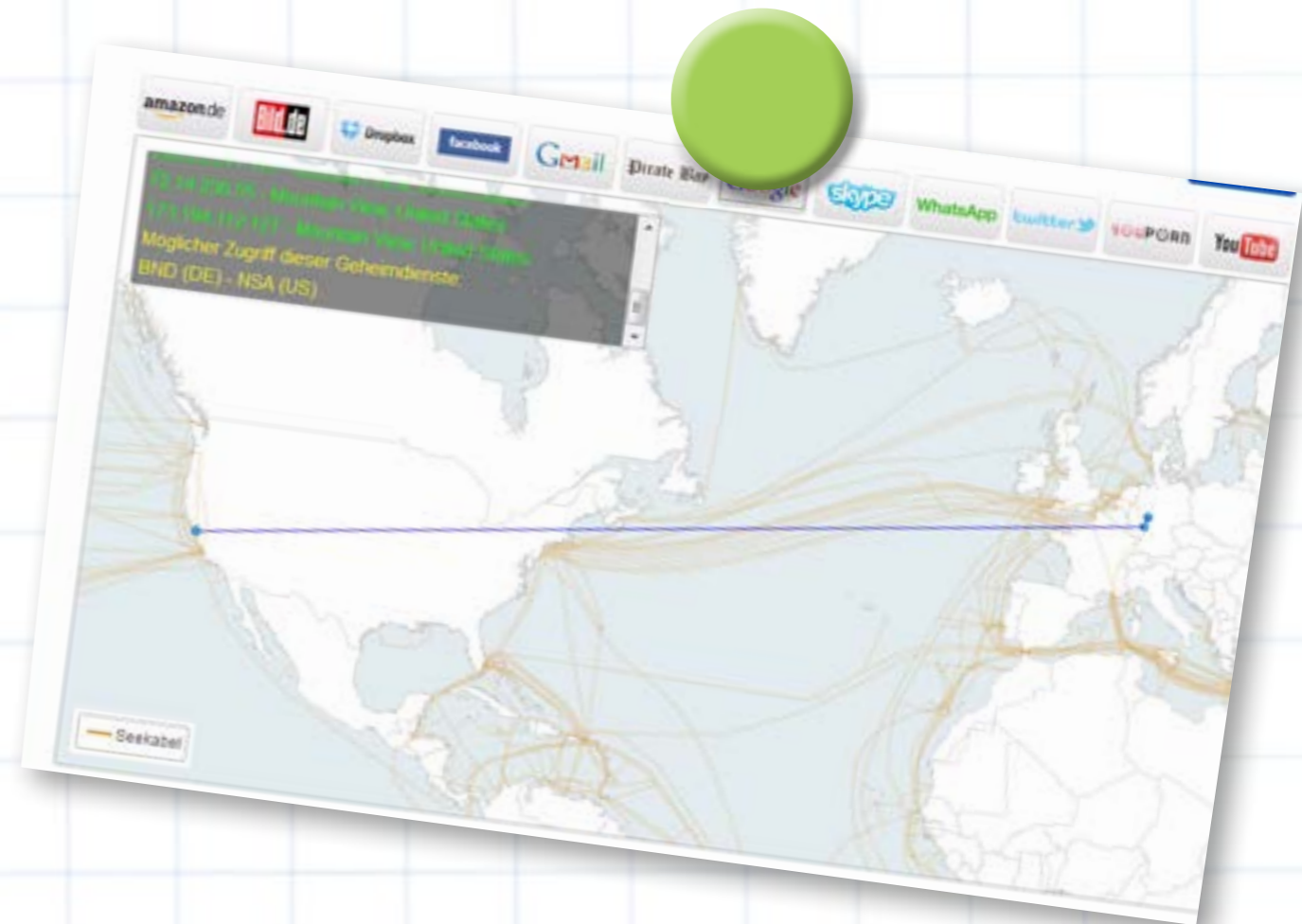
TIPPEN SIE AUF DIE
POST-IT-ZETTEL

Warum Frankfurt?

Frankfurt hat sich in den vergangenen Jahren zum größten Datenumschlagplatz der Welt entwickelt, noch vor Amsterdam und London. Das hat etwas mit dem Aufbau des Internets zu tun: Es besteht aus vielen einzelnen Netzwerken, die miteinander verbunden sind – über Knotenpunkte, von denen es mehr als 300 weltweit gibt. Einer ist in Frankfurt, er besteht aus mehreren Rechenzentren und heißt German Commercial Internet Exchange oder kurz: DE-CIX. Die Betreiberfirma ist eine Tochtergesellschaft des Internetverbandes ECO.

Über den DE-CIX läuft ein großer Teil des deutschen und internationalen Internetverkehrs. Eine App der Journalistenagentur OpenDataCity demonstriert die Bedeutung von DE-CIX, Sie sehen rechts einige Beispiele dafür: Egal, ob Sie Facebook oder Google aufrufen, und selbst wenn Ihr Computer ganz woanders in Deutschland steht, läuft die Anfrage, bis sie ihr Ziel erreicht hat, über mehrere Stationen – und unter anderem über Frankfurt.

„An einem Knotenpunkt laufen sehr, sehr viele Informa-



Der Weg der Daten

Die Journalistenagentur OpenDataCity hat eine App programmiert, mit der Sie ausprobieren können, welchen Weg Ihre Daten gehen, wenn Sie Google oder Facebook aufrufen.

<http://apps.opendatacity.de/prism/de>

Vor dem Knotenpunkt



Wahrscheinlich laufen die Daten über Glasfaserkabel zum Knotenpunkt in Frankfurt - und nicht über Kupferkabel. Deshalb sind zwei Möglichkeiten denkbar, wie sich der Internetverkehr abfangen lasse, erklären Fachleute: Zum einen könne das Glasfaserkabel aufgeschnitten und ein Splitter eingesetzt werden, sagt Josef von Helden, Informatik-Professor an der Hochschule Hannover. „Dann wird der Datenstrom durch das eigene Gerät geleitet und dabei kopiert“, ergänzt Marko Schuba, Professor für Elektrotechnik und Informationstechnik an der Fachhochschule Aachen. Zwar wäre der Datenstrom kurz unterbrochen, während der Splitter eingebaut würde. „Trotzdem muss das Rechenzentrum nicht unbedingt etwas davon mitbekommen, weil kleinere Störungen nicht unüblich sind.“

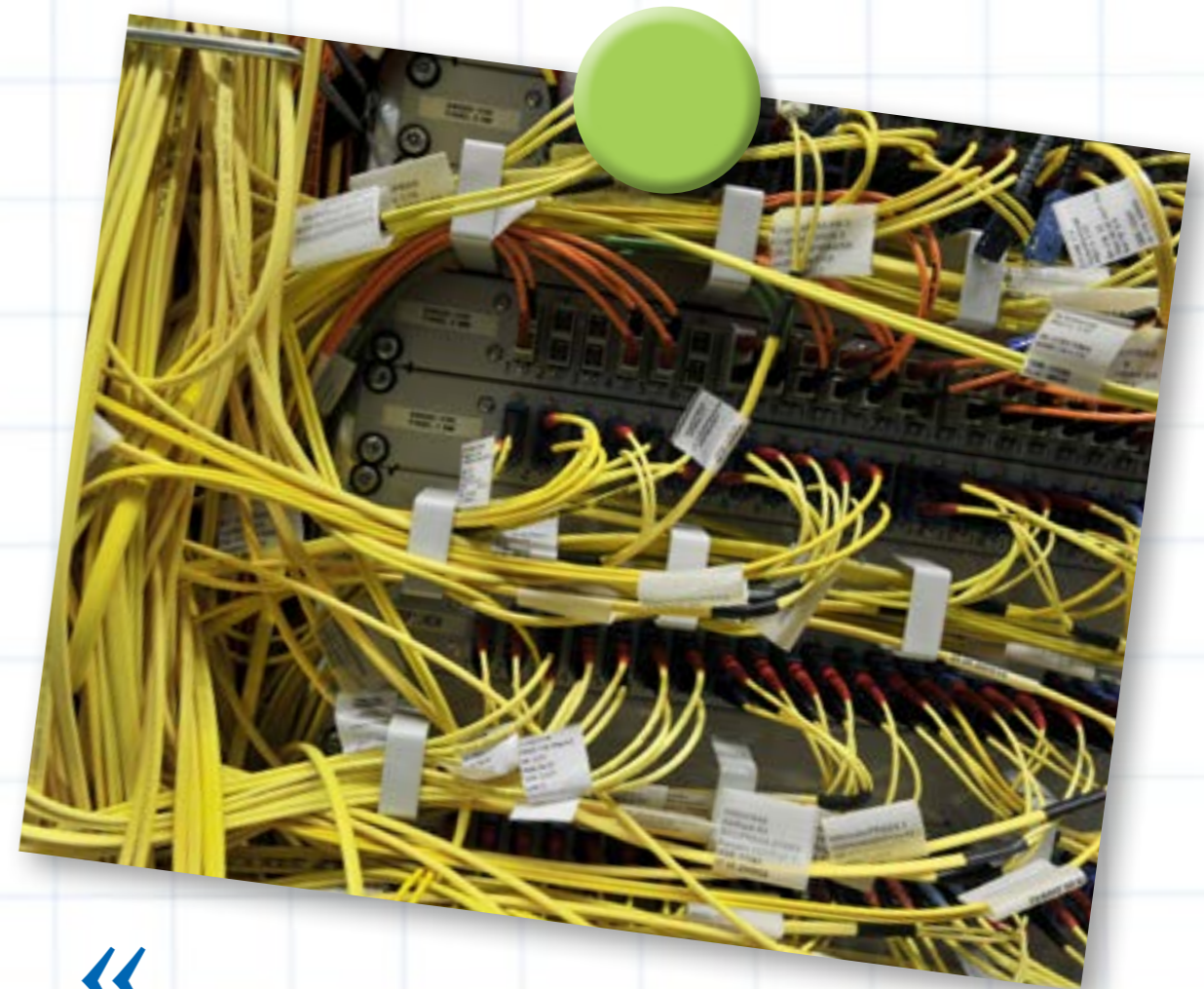
Denkbar wäre auch, das Glasfaserkabel zu biegen, erläutert Schuba. Das Licht folgt zwar



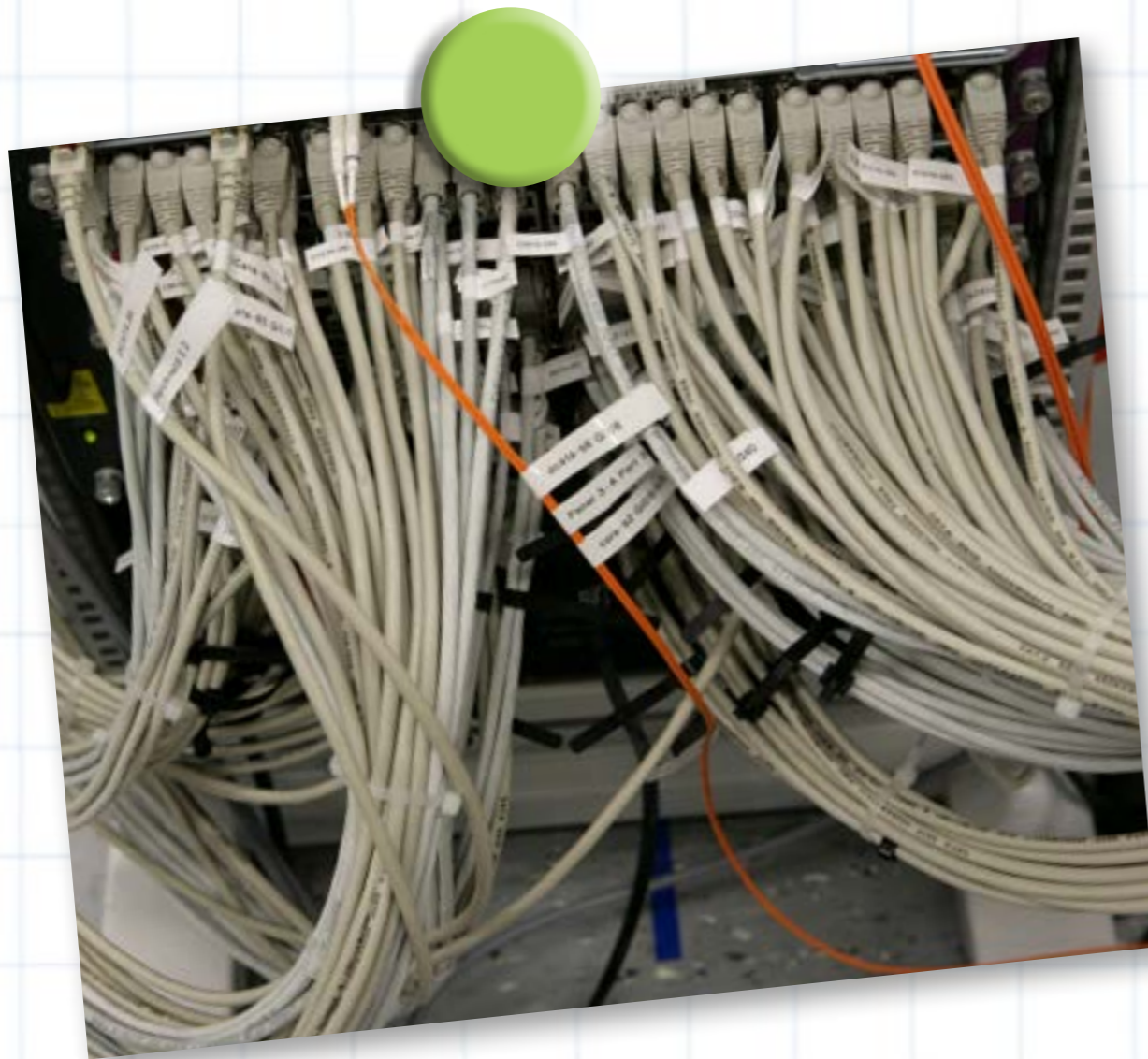
Direkt am Knotenpunkt

Am einfachsten wäre es, am Knotenpunkt selbst, also im Rechenzentrum die Daten mitzuschneiden. Aber wenn hier jemand ein Kabel anklemme und Geräte aufstelle, „müsste das dem Betreiber auffallen“, sagt Josef von Helden, Informatik-Professor an der Hochschule Hannover. Und der Betreiber des Knotenpunktes dementiert vehement, dass die NSA oder andere Auslandsgeheimdienste auf die Datenleitungen zugreifen können. Die für eine Überwachung im großen Stil notwendigen Kabelstränge würden auffallen, sagte ein Sprecher des DE-CIX. Außerdem gebe es verschiedene technische Schutzvorrichtungen.

Ist es wirklich definitiv ausgeschlossen? Es wäre möglich, dass jemand von außen Schadprogramme ins Rechenzentrum einschleuse und die Kontrolle übernehme, sagt von Helden. „Diese Schadprogramme würden weitgehend unbemerkt arbeiten.“ Allerdings könne die Software niemals den gesamten Internet-Traffic umleiten. Deshalb müssten



Hinter dem Knotenpunkt



Durch den Aufbau des Internets ist eine dritte Möglichkeit denkbar: Da es aus vielen einzelnen Netzwerken besteht, also aus Leitungen und Rechenzentren, die nicht den Nationalstaaten, sondern vielen verschiedenen Unternehmen gehören, läuft der weltweite Internetverkehr über die Kabel privater Firmen. Allein am DE-CIX in Frankfurt sind mehr als 500 sogenannte Internet Service Provider angeschlossen. Darunter sind zum Beispiel Telekommunikationsfirmen, Betreiber von Breitbandnetzen und Anbieter von Cloud-Diensten.

Würde nun eines der Unternehmen mit dem US-Geheimdienst NSA zusammenarbeiten, könne die National Security Agency unbemerkt die Daten abfangen, die durch die Leitungen der Firma fließen, erklärt Peter Leppelt, Geschäftsführer der Datenschutzfirma Praemandatum. „Dann kann ich als Geheimdienst die Daten kopieren, und niemand bekommt es mit.“ Deshalb hält auch Josef von Helden, Informatik-Professor