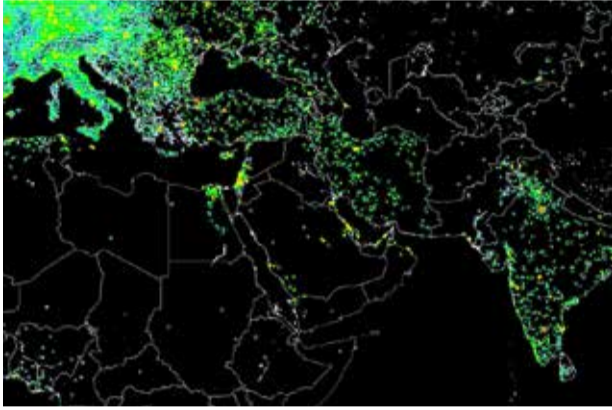


ÜBERWACHUNG UND JOURNALISMUS

# Die Regierungsvertreter waren sich der Ironie nicht bewusst, dass die einzige Organisation, die bislang die Kontrolle über ihre Daten verloren hatte, keine Zeitung, sondern die NSA gewesen war.



VON ALAN RUSBRIDGER, LONDON

Arbeitet eine Zeitung wie der britische «Guardian» an Enthüllungen zu Geheimdiensten – wie jüngst mit Whistleblower Edward Snowden –, so stehen die Agenten bald in der Redaktion und wollen Computer in Fleischwölfe werfen. Der «Guardian»-Chefredaktor über die Schwierigkeit zu verstehen, wie die Überwachung funktioniert, die Ignoranz der parlamentarischen Aufsicht und CEOs voller blindem Vertrauen.

Es ist schwieriger, als man denkt, ein Apple MacBook Pro gemäss den Standards der britischen Regierung zu zerstören. In einer perfekten Welt wünschen die Beamten, die diese Apparate zerstören wollen, dass man sie in einen riesigen Fleischwolf wirft, der sie zu Staub zermalmt. Da der «Guardian» über kein solches Gerät verfügt, erwarben wir am 20. Juli dieses Jahrs eine Bohrmaschine und einen Winkelschleifer und beförderten die Computer unter dem wachsamen Auge zweier staatlicher Beobachter ins Jenseits.

Es war eine harte, staubige Arbeit an jenem Samstag im Untergeschoss des «Guardian», an einem Tag, der sicherlich eine Fussnote in jeder Geschichte darüber verdient, wie in modernen Demokratien Regierungen mit der Presse umspringen. Der britische Staat hatte entschieden, dass «genug» über das Material diskutiert worden sei, das der ehemalige NSA-Angestellte Edward Snowden im Mai öffentlich gemacht hatte. Falls sich der «Guardian» weigere, die Dokumente zurückzugeben oder zu zerstören, dann könne ich, als Chefredaktor, entweder mit einem juristischen Publikationsverbot oder mit einem Besuch der Polizei rechnen – wobei offengelassen wurde, welche der beiden Optionen es sein würde. Der Staat drohte auf jeden Fall damit, die Berichterstattung und Diskussion durch die Presse vorab einzuschränken, unabhängig vom öffentlichen Interesse oder der Bedeutung einer Debatte. Im 18. Jahrhundert war so etwas in Britannien ja gang und gäbe, aber heute eigentlich nicht mehr so ganz.

In unseren Diskussionen mit Regierungsvertretern vor dem 20. Juli hatten wir diesen beizubringen versucht, dass dieses Bestreben, ein Medienunternehmen zu gängeln, nicht nur grundsätzlich falsch, sondern auch sinnlos sei. Selbstverständlich existierten, sagten wir ihnen, weitere Kopien des Snowden-Materials in anderen Ländern. Denn, erklärten wir

ihnen, der «Guardian» arbeite mit Medienunternehmen in den USA zusammen. Glenn Greenwald, der Journalist, der als Erster mit Snowden kooperiert hatte, lebte in Rio de Janeiro. Die US-Filmemacherin Laura Poitras, die ebenfalls mit dem früheren NSA-Angestellten in Kontakt gestanden hatte, besass weiteres Material in Berlin. Was erwarteten sie sich davon, ein paar Festplatten in London zu zerstören? Die Männer von der Regierung sagten, sie seien sich «schmerzlich bewusst», dass weitere Kopien vorhanden seien, aber sie hätten Anweisung, die Aktivitäten des «Guardian» in dieser Sache in London zu beenden, indem sie die Computer zerstörten, die die Informationen von Snowden enthielten.

Ich glaube, unsere Gesprächspartner wussten irgendwie, dass sich das Spiel verändert hatte. Die Technologie, die die Geheimdienstler so begeistert – die ihnen Einblick in das Leben von Milliarden von Menschen erlaubt –, ist zugleich eine Technologie, die praktisch unmöglich kontrolliert oder eingedämmt werden kann. Aber Gewohnheiten lassen sich nur schwer ablegen – deshalb der Rückgriff auf die Gerichte, um eine Veröffentlichung zu verhindern. Sowohl der US Espionage Act von 1917 wie der British Official Secrets Act von 1911 – die beide in Kriegswirren und Spionagefieber wurzeln – werfen einen langen Schatten.

Die USA haben ihre eigenen Schwierigkeiten mit JournalistInnen und deren Quellen. Nichtsdestotrotz herrscht dort ein aufgeschlosseneres Klima für alle, →

die versuchen, eine öffentliche Debatte bezüglich Sicherheit und Schutz der Privatsphäre zu führen, eine Debatte, die, zumindest nach Snowden, offenbar alle für wünschenswert halten.

Der Hauptvorteil in den USA besteht darin, dass es, so hoffe ich, unvorstellbar ist, dass die US-Regierung eine Publikation vorab zu verhindern sucht. Eine geschriebene Verfassung, der erste Verfassungszusatz, der die Meinungsäusserungsfreiheit garantiert, und das Urteil des Obersten Gerichtshofs im Fall der Pentagon-Papers von 1971 haben alle dazu beigetragen, Schutzmechanismen zu errichten, die in Britannien fehlen.

Mit den Snowden-Dokumenten wurde allmählich enthüllt, dass die US- und die britische Regierung in den letzten zehn Jahren in intensiver Zusammenarbeit versucht haben, sämtliche BürgerInnen auf die eine oder andere Art zu überwachen. Das offensichtliche Ziel besteht darin, «jederzeit alle Signale» zu sammeln und zu archivieren – das heisst das vollständige digitale Leben, eingeschlossen Internetabfragen und Telefonanrufe, Texte und E-Mails, die wir machen und einander täglich zusenden.

Wir beginnen auch langsam zu verstehen, wie das gemacht wird. Die National Security Agency (NSA) und das britische Gegenstück, das Government Communication Headquarters (GCHQ), arbeiten eng mit Internetanbietern und Telekommunikationsunternehmen zusammen, um enorme Mengen unserer Daten anzuhäufen.

Manches davon geschieht durch die Eingangstür – durch formale gesetzmässige Anfragen. Manches geschieht näher bei der Quelle bei Hightechfirmen und Telefongesellschaften – indem Signale während der Übermittlung abgefangen werden. Die Geheimdienste haben Apparaturen an Transatlantikkabeln angebracht, die ihnen ermöglichen, Daten von Millionen von BenutzerInnen auf beiden Seiten des Atlantiks abzusaugen. Letztes Jahr bearbeitete GCHQ jeden Tag 600 Millionen «Telefonereignisse», hatte mehr als 200 Fiberglaskabel angezapft und konnte Daten von mindestens 46 von ihnen gleichzeitig verarbeiten.

Wir haben ebenfalls erfahren, wie die Geheimdienste riesige Geldsummen dazu eingesetzt haben, die Integrität des Internets als solches zu unterwandern – indem sie dessen Sicherheit auf eine Weise untergraben, die jede Einzelperson, öffentliche Institution oder Firma beunruhigen sollte, die das Internet benützt. Eine Hintertür, durch die die NSA in Nachrichten eindringen kann, ist, so stimmen die meisten VerschlüsselungsexpertInnen überein, auch durch andere benutzbar. Falls Sie um Ihre Onlinebankdetails oder medizinischen Daten besorgt sind, dann wohl zu Recht.

Das ist alles ziemlich anders als in den Anfängen der modernen Geheimdienste, von denen die meisten, wie die Geheimhaltungsgesetze, die sie beschützen, rund hundert Jahre alt sind. In Britannien begannen sie auf Schuhsohlen – um deutsche SpionInnen zu fangen, die um Schiffswerften herumlungerten. Schon bald versuchten SpionInnen, sich in die neuen Marconi-Kabel der Telegrafie zu hacken. Zeitgenössische Dokumente bezeugen eine weitgehende Ignoranz unter Beamten und Parlamentariern gegenüber den neusten technologischen Entwicklungen. Das Gleiche gilt zweifellos auch heute.

Für den grössten Teil des 20. Jahrhunderts haben wir die Bilder darüber, was SpionInnen tun, von Ian Fleming, John Le Carré oder Robert Ludlum bezogen. Zumeist war es eine Welt, in der Spion gegen Spion antrat. Bei der dabei eingesetzten Technologie handelte es sich um Technospielzeug: Pistolen mit raketentriebener Munition, gefälschte Fingerabdrücke, Zigaretten mit Tränengas oder explodierende Zahnpasta.

Unsere Vorstellungskraft ist unweigerlich durch George Orwell gefärbt, der zwar keine Spionageromane schrieb, aber eine verstörende Vision entwarf, wie Technologien, die jeden Winkel ausleuchten, eine Gesellschaft in dunkle Sackgassen führen könnten.

Edward Snowden, ein 29-jähriger NSA-Mitarbeiter, der in Hawaii lebte, hatte eine bessere Sicht auf das, was Geheimdienste heutzutage so treiben – und dies ähnelt nur wenig der Welt von Flemings 007 oder George Smiley, dem Helden von Le Carré. Snowden hatte Zugang zu Millionen als geheim klassifizierter Dokumente und Einsatzbesprechungen sowohl der NSA wie des GCHQ. Was er sah, beunruhigte ihn zutiefst: «Selbst wenn man nichts Unrechtes tut, wird überwacht und aufgezeichnet, was man tut», sagte er dem «Guardian», als er sich als derjenige zu erkennen gab, der Anfang Juni geheimes Material öffentlich gemacht hatte. In einem Videointerview erklärte er: «Die Speicherkapazität dieser Systeme erhöht sich jedes Jahr in einer Grössenordnung, mit der man an einen Punkt kommt, wo man gar nichts Unrechtes mehr getan haben muss. Man muss bloss irgendwie in Verdacht geraten, und sei es, indem man eine falsche Telefonnummer wählt. Dann können sie das System benutzen und rückblickend jede Entscheidung durchstöbern, die man

je gemacht hat, jeden Freund, mit dem man je etwas diskutiert hat. Und sie können einen aufgrund eines solcherart abgeleiteten Verdachts in einem ganz unschuldigen Leben angreifen und in die Nähe eines Übeltäters rücken.»

Um seinen eigenen Entscheid zu erklären, weshalb er zum Whistleblower, zum Informanten, geworden sei, mit all den entsprechenden Konsequenzen, die das für den Rest seines Lebens haben würde, fügte er hinzu: «Man merkt, dass das die Welt ist, die du mit geschaffen hast, und es wird mit der nächsten Generation schlimmer werden und mit der übernächsten noch schlimmer, um das Potenzial dieser Architektur der Unterdrückung weiter auszubauen.»

In Snowdens Sicht sind die herkömmlichen Formen der Kontrolle – geheim tagende, einseitig zusammengesetzte Gerichte und geschlossene Komitees des US-Kongresses oder des britischen Parlaments – ungenügend. Nicht zuletzt weil sie nur über beschränkte Informationen verfügen, die Technologien kaum verstehen und häufig falsch informiert werden. Da er diesen Gerichten und dem Kongress nicht traute, kontaktierte Snowden jene anderen Menschen, die in einer modernen Demokratie dazu da sind, die Wahrheit zu enthüllen, Debatten zu initiieren und Personen zur Verantwortung zu ziehen – JournalistInnen.

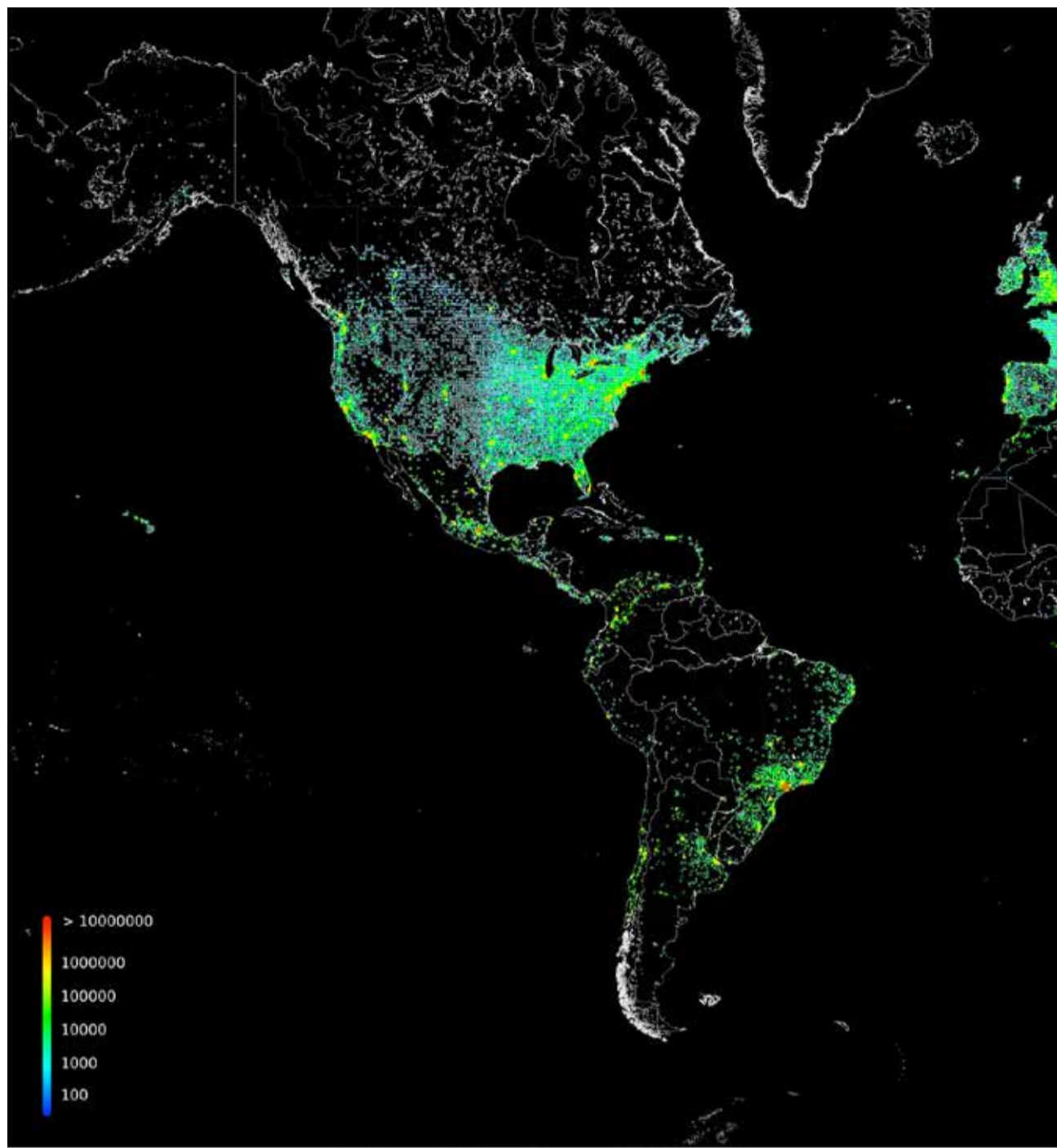
Aber zurück ins Untergeschoss des «Guardian», zur heissen, staubigen Arbeit, einen Computer zu zertrümmern. Warum waren wir dort?

Eine scheinbar einleuchtende Antwort ist jene, die uns die Regierung gab: dass es für den «Guardian» nicht sicher sei, in einem Redaktionsbüro hoch geheime Dokumente zu untersuchen, welche Vorsichtsmassnahmen wir auch immer treffen würden.

Tatsächlich standen wir diesem Argument mit einer gewissen Sympathie gegenüber: Wir waren auch nicht auf zufällige weitere Lecks erpicht. Die Regierungsvertreter, die uns belehrten, waren sich allerdings der Ironie nicht bewusst, dass die einzige Organisation, die bislang nachweislich die Kontrolle über ihre Daten verloren hatte, keine Zeitung, sondern die NSA gewesen war.

Eine einleuchtendere Antwort lautet, dass es die britischen Geheimdienste extrem schwierig finden, mit JournalistInnen umzugehen. Was das übergreifendere Problem illustriert, Überwachung mit zivilen Rechten auszubalancieren. Wie in aller Welt vereint man etwas, das geheim bleiben sollte, mit etwas, das diskutiert werden muss?

Mit den fortschreitenden Enthüllungen von Snowden wurde offensichtlich, wie stark die Geheimdienste von kommerziellen Dienstleistungen abhängig sind, die wir alle benutzen – Internetanbieter, Telefongesellschaften und soziale



Das Internet, der riesige Heuhaufen des goldenen Zeitalters der Überwachung: Lokalisierung aller Rechner, die auf eine

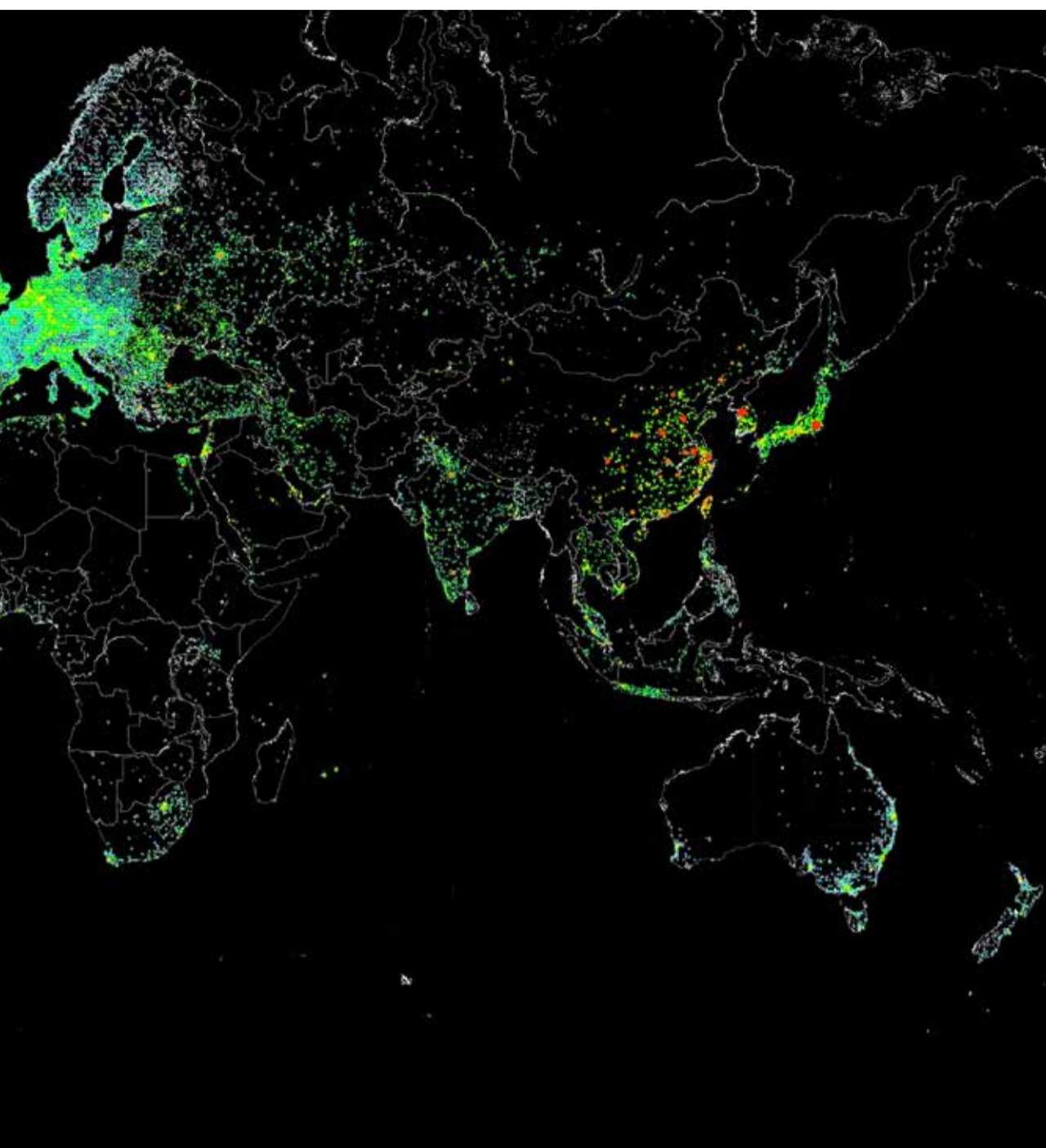
Netzwerke –, sowohl auf offiziellem wie auf inoffiziellem Weg.

In den USA wie in Britannien ist der Mantel der gesetzlichen Geheimhaltung um diese Aktivitäten so geschneidert, dass keine dieser Firmen sich traut, offen über ihre Beziehung mit den Geheimdiensten zu reden. So etwas ist ja illegal. Andererseits befürchten die Regierungen auf beiden Seiten des Atlantiks, dass Privatunternehmen das Weite suchen, wenn die KonsumentInnen erfahren, wie entgegenkommend die Firmen mit ihren Daten umgehen.

Ich hatte ein interessantes Gespräch – selbstverständlich «off the record» – mit einem ziemlich hohen Kader eines der Riesenunternehmen an der US-Westküste: Er gestand ein, dass weder er noch der CEO seiner Firma berechtigt waren, die Abkommen seiner eigenen Firma mit der US-Regierung einzusehen. «Dann gibt es also ein Unternehmen innerhalb des Unternehmens?», fragte ich. Er wedelte abwehrend mit der Hand: «Ich kenne den Typen, ich traue ihm.»

Es braucht offenbar ziemlich viel Vertrauen in jener Welt, von der Edward Snowden den Vorhang zurückgezogen hat. Wer die Dienste dieser speziellen Firma beansprucht, hat einem anonymen Mann (nicht dem CEO) zu trauen, dass der eine verlässliche Beziehung mit der Regierung habe (die nicht die Regierung des Kunden zu sein braucht). Andere Dokumente, die wir gesehen haben, zeigen, dass gewisse Telekommunikationsfirmen «ziemlich weit» über das hinausgehen, was sie gesetzlich zu tun verpflichtet wären.

Kein Wunder, schickte der Staat seine Vertreter in Redaktionsbüros, um die ChefredaktorInnen zu überzeugen, den Deckel auf diesem ganzen Gebräu draufzulassen. Die Argumente sind die erwartbaren: Ihr habt Blut an euren Händen, denn



globale IP-Anfrage reagiert haben (2012). QUELLE: CARNA BOTNET

unsere Welt wird «im Chaos versinken».

Dieses Argument ist vom US-amerikanischen Rechtsprofessor Peter Swire fachgerecht zerpfückt worden. Swire beriet einst Bill Clinton in Fragen des Datenschutzes und sitzt gegenwärtig in der Untersuchungskommission von Barack Obama zur NSA. In einem 2011 veröffentlichten Essay zeigt er, dass FBI und NSA seit den neunziger Jahren jammern, ihre Überwachungsmöglichkeiten würden sich wegen der vergrößerten Verschlüsselungsmöglichkeiten im Internet verringern. Nachdem Swire erklärt hat, warum Verschlüsselung «für das wirtschaftliche Wachstum, die individuelle Kreativität, Staatsgeschäfte und zahlreiche andere Ziele» wichtig ist, fordert er die US-AmerikanerInnen dazu auf, solcherlei Proteste von Regierungsseite skeptisch zu betrachten: «Aufgrund der veränderten Technologien verlieren Strafverfolgungsbehörden und nationale Geheimdienste tatsächlich frühere einschlägige Potenziale. Diese Verluste werden allerdings durch massive Gewinne mehr als aufgewogen. Die Öffentlichkeit sollte erkennen, dass wir in einem für die Überwachung goldenen Zeitalter leben. Verstehen wir das, können wir auch die Forderungen nach einer bewusst lückenhaften Verschlüsselungspolitik zurückweisen. Wir sollten überhaupt grundsätzlich viele Vorschläge kritisch betrachten und eine sicherere Computer- und Kommunikationsinfrastruktur aufbauen.»

Ein Editorial im «Economist» hat kürzlich ebenfalls die Bedeutung der alarmierenden NSA-Politik erkannt, die Integrität des ganzen Internets zu schwächen. «Jede bewusste Untergrabung der Verschlüsselungssysteme durch die NSA ist schlicht und einfach eine schlechte Idee und sollte aufhören. Sicher würde dadurch das Leben für die regierungsamtlichen SchnüfflerInnen erschwert. Aber es gibt jede Menge gezielt einsetzbarer Instrumente, die sie verwenden können und die nicht die Sicherheit für alle NutzerInnen des Internets reduzieren, den Ruf der US-Technologieindustrie ramponieren und die Regierung unglaubwürdig und unaufrichtig aussehen lassen.»

An dieser Stelle muss ich gestehen: Ich habe diese in den NSA- und GCHQ-Dokumenten versteckte Geschichte – dass die Strafverfolgungsbehörden die Möglichkeiten der privaten Verschlüsselung unterminieren – nicht selbst aufgespürt; selbst als sie mir junge, auf diese Technologien spezialisierte Reporter, die ihre Bedeutung erkannt hatten, zu erklären versuchten, verstand ich sie nicht sofort. Peinlicherweise musste ich eine Art Kinderzeichnung anfertigen, um mir bestätigen zu lassen, was ich glaubte, von ihnen erzählt bekommen zu haben.

Verfügen US-amerikanische und britische ParlamentarierInnen über ein besseres Verständnis darüber, was die heutige Technologie vermag? Können sie, als angebliche Regulator-

Innen, solche Dokumente ebenfalls entziffern?

Damit sind wir wieder beim Vertrauen angelangt. Falls Zeitungen diese Dinge nicht aufdecken, analysieren und erklären, müssen wir darauf vertrauen, dass Parlamentskomitees oder geheime, einseitig zusammengesetzte Gerichte die Arbeit für uns erledigen.

In den USA befinden wir uns weitgehend in den Händen von Senatorin Dianne Feinstein und in Britannien in denjenigen von Malcolm Rifkind, einem ehemaligen Verteidigungsminister. Beide sind, um es freundlich auszudrücken, keine Kinder des digitalen Zeitalters. Vielleicht tue ich Feinstein und Rifkind ja unrecht, aber sie hätten wohl Mühe gehabt, die Dokumente zu verstehen, die mir Jeff entzifferte – mit oder ohne meine Zeichnung als Hilfe. Wir hören hier, hundert Jahre später, den Widerhall der Whitehall-Bürokraten, die damals versuchten, die Marconi-Kabel zu knacken.

Die nun von Snowden zugänglich gemachten Dokumente zeigen, dass NSA und GCHQ extrem talentierte TechnikerInnen beschäftigen, die immer erfindungsreicher immer exotischere Wege aushecken, um Millionen von Menschen zu beobachten. Wenn man ihre Methoden unter die Lupe nimmt oder sogar darüber schreibt, wird routinemässig geantwortet, wir lieferten uns damit unseren Feinden aus.

Unsere SchnüfflerInnen beharren darauf, innerhalb des gesetzlichen Rahmens zu agieren. Sie erklären einem geduldig den Unterschied zwischen einem Heuhaufen – den sie auf jeden Fall anhäufen dürfen – und einer Stecknadel, nach der sie nur unter ganz bestimmten Umständen suchen dürfen.

Niemand bezweifelt, dass ihre Aufgabe wichtig ist. Wir brauchen fähige Geheimdienste. Freiheitliche Demokratien haben entschlossene und findige GegnerInnen. Doch offen-

sichtlich besteht eine Spannung zwischen der Geheimhaltung, die manche nachrichtendienstliche Tätigkeit braucht, und der Offenheit, die eine Demokratie in allen anderen Angelegenheiten verlangt. Sorgfältiger, verantwortungsvoller Journalismus ist ebenso notwendig. «The Guardian», «The Washington Post», «Pro Publica» und «The New York Times» haben alle Vorsorge getroffen, das Material von Snowden verantwortungsvoll zu veröffentlichen. Privat – aber natürlich nicht öffentlich – räumen jene, die mit dem Material vertraut sind, das auch ein.

Diese übergreifende Frage nach dem Verhältnis von Geheimhaltung und Offenheit ist so wichtig, weil die Polizei und die Geheimdienste (und andere) mit der sich entwickelnden Technologie immer mehr und grössere Heuhaufen fordern – und die Möglichkeit, sie immer länger zu konservieren; sowie die Möglichkeit, erstaunlich wirkungsvolle Algorithmen zu entwickeln, um die Nadeln zu finden. Gegenwärtig sind in Britannien schätzungsweise rund fünf Millionen Überwachungskameras im öffentlichen Raum installiert. Es ist sicherlich bloss eine Frage der Zeit, bis jemand vorschlägt, diese Kameras mit Software zur Gesichtserkennung auszustatten (und zwar von jener Art, die selbst Google gegenwärtig noch nicht freizugeben wagt) und vielleicht auch noch gleich Strassenmikrofone zu installieren, damit sich zusätzlich Gespräche aufnehmen lassen.

Das würde – argumentieren diese Leute zweifellos – den «good guys» helfen, die «bad guys» im Auge zu behalten und vielleicht einen weiteren Terroranschlag auf britischem Boden verhindern. Und jemand wird einem künftigen Chefredaktor sicherlich erklären: «Schreiben Sie darüber, und Sie haben womöglich Blut an Ihren Händen. Denn Terroristen werden damit beginnen, die Hauptstrassen und andere Stellen mit Überwachungskameras zu meiden. Unsere Welt wird im Chaos versinken.»

Verschiedene bekannte Intellektuelle und RechtsanwältInnen bezweifeln zutiefst, dass die jetzigen Aufsichtsmaßnahmen funktionieren können. Der frühere Appellationsrichter Sir Stephen Sedley beschrieb kürzlich in der «London Review of Books» seine Verzweiflung über «ein gesetzlich abgesichertes Überwachungsregime, das sich in Geheimhaltung übt und Teil eines wachsenden Verwaltungsregimes ist, das einige von uns daran zweifeln lässt, ob die traditionelle Gewaltentrennung – Legislative, Justiz, Exekutive –, die traditionellerweise von John Locke, Charles de Montesquieu und James Madison hergeleitet wird, immer noch funktioniert. Der Sicherheitsapparat ist heutzutage in manchen Demokratien fähig, eine Macht über die anderen Teile des Staats auszuüben, die zuweilen an Selbstregierung grenzt: Er treibt Gesetzgebungen voran, die seine eigenen Interessen über die Individualrechte setzen, er prägt Entscheide der Exekutive, schliesst GegnerInnen aus dem Rechtsprechungsprozess aus und funktioniert praktisch jenseits jeder öffentlichen Aufsicht. Der (noch vor dem 11. September 2001 eingeführte) Terrorism Act – auf dessen Grundlage kürzlich David Miranda, der Freund des Edward-Snowden-Kontaktmanns Glenn Greenwald, am Londoner Flughafen Heathrow verhaftet wurde – ermöglicht den willkürlichen Einsatz umfassender Vollmachten zur Befragung, Durchsuchung und Internierung. Er veranschaulicht einen langfristigen Trend, sowohl was verfassungsmässig zulässig als auch was verfassungsmässig akzeptabel ist. Ersteres mag eine Sache fürs Parlament sein; Letzteres aber geht weiterhin uns alle an.»

Ich denke, er hat recht.

Aus dem Englischen von Stefan Howald.

© 2013 The New York Review of Books /  
Distributed by The New York Times Syndicate

## Linksliberales Gewissen



Wegen der Snowden-Enthüllungen ist der «Guardian»-Chefredaktor Alan Rusbridger unter massiven Druck der britischen Geheimdienste geraten und soeben vor einen Ausschuss des britischen Parlaments vorgeladen worden. In den letzten Jahren produzierte die linksliberale Zeitung immer wieder aufsehenerregende Enthüllungen. Seit 2007 arbeitet sie mit der Enthüllungsplattform WikiLeaks zusammen und hat jeweils deren wichtigste Dokumente veröffentlicht, etwa 2010 die Depeschen von US-amerikanischen Botschaften. Bei den Enthüllungen von Edward Snowden gehört der «Guardian» zum Konglomerat jener Zeitungen, die das Material weltweit aufbereiten und publizieren.

Geleitet wird das Traditionsblatt seit 1995 von Alan Rusbridger (59). Der setzt neben der Printausgabe dezidiert auf das Internet; die «Guardian»-Website mit einem umfangreichen Archiv und vielen interaktiven Elementen ist eine der meistgelesenen der Welt, fährt aber durch die Gratisbenutzung massive Verluste ein. Der hier abgedruckte Artikel erscheint in erweiterter Form in der «New York Review of Books» vom 21. November 2013.