Julian würde die Liste ohne Zögern publik machen

Julian Assange prophezeite 2012 im Buch „Cypherpunks“, die globale Zivilisation werde binnen weniger Jahre in einen postmodernen Überwachungsalptraum schlittern. Der Investigativ-Journalist Jacob Appelbaum, der momentan über angewandte Kryptographie an der Eindhoven University of Technology forscht, war damals einer von Assanges Co-Autoren und hatte bereits mit WikiLeaks zusammengearbeitet. Später war er an der Analyse der von Edward Snowden enthüllten Machenschaften der amerikanischen National Security Agency (NSA) beteiligt. Sind die Enthüllungen, die uns jetzt über das Spähprogramm Pegasus, seine Käufer und die ausgespähten Personen erreichen, vergleichbar mit denen Assanges und Snowdens? Und wie geht das „Pegasus Project“, eine Gruppe aus Medienunternehmen und Amnesty International, mit dem geleakten Material um? Nicht nur vorbildlich, findet Appelbaum.

VON ANGELA RICHTER

DIE WELT: Mr. Appelbaum, woher stammen die geleakten Telefonnummern aus dem Pegasus-Projekt?
JACOB APPELBAUM: Es kursieren verschiedene Geschichten. Aber es klingt so, als ob der Ursprung in Zypern liegt. Unklar ist aber, was das bedeutet. Die Liste soll ja fünfzigtausend Telefonnummern enthalten.

Warum weiß man trotz der enormen Berichterstattung so wenig Genaues?
Die Leute vom Pegasus-Projekt halten mit den Details extrem hinter dem Berg. Sie möchten es wohl anders machen als Wikileaks, wo man alles transparent offenlegen würde. Das ist ziemlich frustrierend, wenn man davon ausgeht, dass die NSO-Gruppe etwas grundlegend Falsches tut, so aber geschützt bleibt.

Was genau kritisieren Sie am Pegasus-Projekt?
Ich finde es schockierend, dass sie all diese Telefonnummern haben und alles, worüber berichtet wird, Geschichten über berühmte Leute sind, die betroffen sind. Was ist mit all denen auf der Liste, die vielleicht nicht berühmt sind? Die meisten der Pegasus-Opfer werden vermutlich nie herausfinden, dass sie überwacht wurden.

Wie könnte man es denn besser machen?
Man könnte zum Beispiel eine Webseite einrichten, auf der jeder seine Telefonnummer eingeben kann, und man benachrichtigt wird, wenn die sich im Datensatz befindet.

Und warum macht man das nicht einfach?
Ein Grund dafür könnte sein, dass Amnesty International involviert ist. Amnesty ist sehr darauf bedacht, seine Marke als Menschenrechtsorganisation zu schützen. Amnesty kann das Risiko nicht eingehen, versehentlich mit den Informationen auch einem “Schurkenstaat” oder “Bösewicht” einen Vorteil zu verschaffen. Das hat nichts mit Moral zu tun. Es ist einfach Pragmatismus. Dann gibt es die „Forbidden Stories“-Gruppe aus Frankreich, das Medienunternehmen, das laut BBC diese Geschichten koordiniert hat. Sie spielten dabei im Grunde die Rolle, die in ähnlichen Fällen WikiLeaks übernommen hat. Offenbar haben sie irgendwie Zugang zu dieser Liste bekommen. Dann haben sie alle Medienpartner und Amnesty koordiniert. Mein Eindruck ist, dass das Leute sind, die Angst haben, ein “bisschen zu weit” zu gehen. Wenn mir jemand diese Liste zuspielen würde, würde ich keine Sekunde zögern, sie zu veröffentlichen. Und wenn Julian ...

... Julian Assange.
Wenn er in Freiheit wäre, würde er dasselbe tun.

Das wäre riskant!
Vorher müsste man natürlich sicherstellen, dass jeder auf der Liste benachrichtigt oder identifiziert wird. Und das ist eine Heidenarbeit! Aber das Problem ist, dass die NSO-Gruppe in der Zwischenzeit an alle auf der Liste ein “Update” rausschicken könnte.

Wozu?
Sie könnten so aus der Ferne Daten auf den Telefonen löschen, um forensische Spuren zu verwischen.

Und wie verhindert man das?
Es wäre wichtig, die Daten erst einmal zu sichern. Das heißt, man muss jede einzelne Person auf der Liste anschreiben: „Hi! Wir sind von Amnesty International. Wir glauben, dass Ihr Telefon von der NSO-Gruppe kompromittiert worden ist. Wir werden das veröffentlichen, aber wir brauchen Sie, um die Beweise zu sichern. Bitte notieren Sie sich diese URL, füllen Sie das Formular aus, schalten Sie Ihr Telefon aus und nicht wieder ein, bis wir es analysiert haben.“ So etwas in der Art. Und dann bekommen sie fünfzigtausend Telefone zum Analysieren. Okay, das ist eine Menge Arbeit, aber sehen Sie, nur dieser Ansatz garantiert, dass alle fünfzigtausend Leute informiert werden und keine Beweise vernichtet werden. Meinem Verständnis nach ist das nicht passiert.

Wie geht das Pegasus-Projekt stattdessen vor?
Ich habe einige Daten zu sehen bekommen, die darauf hindeuten, dass sie die Telefonnummern nur Stück für Stück durchgehen. Jedes Recherche-Team führt seine eigenen Recherchen zu der Liste durch. Sie suchen nach Telefonnummern, die ihnen bekannt sind, und sehen, ob diese in der Liste auftauchen. Und bei einem Treffer sagen sie: ”Hey, schau mal, das ist die Prinzessin von Dubai!”

Was ich noch nicht verstanden habe: Ist die NSO-Gruppe selbst direkt an der Spionage beteiligt?
Das ist eine interessante Frage. Die NSO-Gruppe hat ja gesagt, Pegasus sei wie ein Auto und sie seien nur wie die Hersteller, die es verkaufen. Wenn jemand ein Auto stiehlt oder betrunken einen Unfall baut, ist das sein Problem. Sie werden dann doch den Autobauer nicht zur Verantwortung ziehen, oder?

Wie beurteilen Sie das?
Das ist ein ziemlich schwacher Vergleich. Die NSO-Gruppe lehnt jede Verantwortung dafür ab, wie ihr Produkt genutzt wird. Aber sie behauptet auch, dass die Kunden im Durchschnitt nur hundert Leute ins Visier nehmen, es gäbe keine Liste mit fünfzigtausend Leuten und so weiter. Gleichzeitig beharren sie darauf, dass sie keinen Einblick in die Zielpersonen ihrer Kunden haben. Wenn sie aber wissen, dass es nur hundert Zielpersonen pro Kunde sind, wirft das die Frage auf, woher sie das wissen. Ed Snowdens Analogie ist da wesentlich treffender. Er sagte, dass ein ganzer IT-Sektor - die israelische Firma NSO ist ja nur ein Beispiel von vielen - ein einziges Produkt anbietet: Software-Exploits, also Viren.

Snowden sagt, dass dieses Unternehmen für das Virus, das es verbreitet, keine Impfung anbietet.
Wenn die NSO-Gruppe weiß, dass hundert Menschen ins Visier genommen werden von einem Kunden, dann deutet das darauf hin, dass sie mehr Einblick in die Zielpersonen ihrer Kunden hat, als sie behaupten. Jemand hat einen Server, gibt Ihre Telefonnummer ein und drückt einen Knopf, um Ihr Telefon zu kontrollieren. Wenn das erfolgreich war, verbindet sich Ihr Telefon mit dem, was die Befehls- und Kontrollinfrastruktur ist, die vielleicht von der NSO-Gruppe betrieben wird. Oder von den Kunden selbst. Es ist ein wenig unklar, wie das aufgesetzt ist – es hört sich so an, als ob die NSO-Gruppe involviert ist, aber natürlich äußert sie sich dazu nicht ganz transparent. Wir wissen es also nicht wirklich. Genauso wenig wie wir wissen, woher diese Liste mit fünfzigtausend Telefonnummern kommt. Was wir wissen ist, dass die NSO-Gruppe damit eine Menge Geld verdient und dass es eine Menge offener Fragen gibt.

Ist die NSO-Gruppe nun für die eigentliche Spionage zur Verantwortung zu ziehen?
Nun, wenn die NSO-Gruppe Pegasus nicht entwickelt hätte, gäbe es überhaupt keine Spionage durch diese Software. Es beginnt und endet also mit der NSO-Gruppe, egal was sie da nun genau tut oder nicht. Es sieht zum Beispiel so aus, als wären amerikanische und israelische Telefonnummern von der Überwachung durch die Pegasus-Software ausgenommen, diese Telefonnummern funktionieren dann einfach nicht. Abgesehen davon scheint es keine Vorsichtsmaßnahmen von Seiten NSOs zu geben, dass zum Beispiel ein Staatsoberhaupt wie der französische Präsident nicht überwacht werden darf. Die NSO behauptet zwar, dass Menschenrechtsanwälte und Journalisten tabu sind, aber soweit ich das beurteilen kann, haben sie die Technologie nicht so gestaltet, dass Menschenrechtler und Journalisten ihre Nummer bei NSO registrieren können, damit sie nicht ins Visier genommen werden. Wahrscheinlich gibt es aber Gebrauchsanweisungen für Kunden, wo erklärt wird, was sie tun müssen – zum Beispiel, dass sie Emailadressen und Telefonnummern der Ziele besorgen müssen, und so weiter. Und dann, wenn sie die haben, geben sie die in die NSO-Software ein. Die NSO-Gruppe muss also die Leute schulen. Direkt oder indirekt, letztendlich ist das Geschäftsmodell der NSO-Gruppe Spionage.

Weiß die NSO-Gruppe, auf wen ihre Spyware Pegasus angesetzt wird? Wie schützen wir uns vor der Überwachung? Jacob Appelbaum hat Antworten

Ist das Pegasus Leak mit den Snowden-Leaks über die Machenschaften der NSA vergleichbar?
Nun, ich würde es eher mit den Panama Papers vergleichen. Snowden hat uns gezeigt, wie die Geheimdienste weltweit zusammenarbeiten und uns ausspionieren. Wir verstehen Massenüberwachung jetzt ganz anders als vor Snowden. Die Enthüllungen rund um Pegasus und NSO sind vielleicht vergleichbar mit den Panama Papers in dem Sinne, dass gesagt wird: „Wir haben diesen unglaublichen Datensatz und wir haben ihn studiert, hier ist die Story!“ Aber wie bei den Panama Papers bekommt man die Original-Dokumente nicht zu sehen, denn dann könnte man sich ja selbst ein Bild davon machen und selbst recherchieren.

Bei den Snowden-Leaks konnte man das?
Wir haben uns wirklich bemüht, sicherzustellen, dass man genau das tun konnte. Es war sehr wichtig für Laura Poitras, Glenn Greenwald, mich und andere Beteiligte, dass jeder verstehen konnte, was die NSA da macht. Jeder der wollte, hatte Einblick in die Dokumente, in die journalistischen Recherchen und die Gespräche mit den Quellen. Die Beweise waren unbestreitbar, sogar für die Regierungen selbst. Und wenn die versuchten, zu lügen, haben wir sofort ein Dokument veröffentlicht, das die Lüge entlarvt hat. Es war ganz anderes als das, was ich beim Pegasus-Leak sehe. Was ich da sehe, ist, dass Amnesty einen guten Namen hat, wie auch einige der Medien, die beteiligt sind. Und sie haben sehr gute technische Leute bei Amnesty, die wirklich wissen, was sie tun, und sie sind mit ihren Analysen transparent. Insofern ist das Vorgehen besser als bei den Panama Papers. Amnesty hat sogar Tools entwickelt, mit denen man seine eigenen Geräte daraufhin überprüfen kann, ob sie von der NSO-Software befallen wurden oder nicht. Das ist ein wichtiger Schritt.

Sie und Assange haben sich schon vor Jahren mit Massenüberwachung befasst. Wie gingen Sie da vor?
Der Pegasus-Leak ist vielleicht am ehesten vergleichbar mit den WikiLeaks Spyfiles-Publikationen. Vor etwa zehn Jahren haben wir uns alle zusammengetan und daran gearbeitet, die milliardenschweren privaten Spionageunternehmen in den Blick zu nehmen. Wir haben das „Wall Street Journal“ mit ins Boot geholt und mit einer ganzen Reihe verschiedener Medienpartnern zusammengearbeitet. Eine meiner Lieblingsaufgaben dabei war, dass ich zu Überwachungsmessen ging, auf denen Vorläufer der NSO-Gruppe ihre Waren verkauften. Ich habe mit ihnen Verkaufsgespräche geführt, als potenzieller Kunde, und so sammelte ich alle Arten von Informationen. Die Pegasus Leaks gehen nicht so weit. Die Sache hat zwar geopolitische Aspekte, die vergleichbar sind. Aber im Moment prügeln alle auf den NSO ein. Das ist besonders einfach, weil die Abneigung gegen Israel im Moment so groß ist. Aber die Realität ist: Was die NSO- Gruppe tut, ist nicht anders als das, was die US-Firma Verint tut und viele andere auch. Es ist nicht anders als das, was NSA und CIA tun. Wenn überhaupt, dann ist ein wesentlicher Unterschied, dass die NSO-Gruppe sich nicht als ein feindlicher Geheimdienst tarnt, also zum Beispiel versucht, den Russen oder Chinesen die Schuld in die Schuhe zu schieben, so wie es das US-Militär und die Geheimdienste tun, was Wikileaks im Vault 7-Leak enthüllt hat. NSO steht immerhin offen zu seinen Geschäften.

„Forensic Architecture“ und auch Ihre Freundin Laura Poitras haben Pegasus schon künstlerisch verarbeitet. Warum wird jetzt erst so groß berichtet?
In der Snowden-Ära war im Westen der Tenor: Auch wenn diese Jungs vielleicht Regeln brechen und ein bisschen zu weit gehen, es sind immer noch die Guten, es sind unsere Jungs! Ich denke, dass es jetzt bei NSO ein geopolitisches Element gibt: Im Grunde haben die Israelis nicht das gleiche Maß an geopolitischer Unterstützung. Die Aufmerksamkeit für den Fall spiegelt auch eine Verschiebung im Diskurs über Israel und Palästina wieder. Es wäre möglich, die NSO-Gruppe im Westen unschädlich zu machen. Zum Beispiel könnte die Software in allen NATO-Ländern für illegal erklärt werden. Dann könnte man Druck auf Israel ausüben, nicht an Nicht-NATO-Länder zu verkaufen. Oder man könnte das Gegenteil tun und sagen, die NSO-Gruppe darf nur an NATO-Länder verkaufen, sonst nirgendwohin. Ich vermute, ein Teil dessen, was vor sich geht, hat damit zu tun, dass es wenig Hemmungen gibt, den Staat zu kritisieren, in dem diese Leute leben und arbeiten. Als die Snowden-Sache herauskam, gab es Leute, die sagten, die Massenüberwachung verstößt gegen internationales Recht. Aber es gab auch die Gegenseite, die meinte, naja, wissen Sie, diese Werkzeuge werden von legitimen Behörden benutzt. Ich beobachte jetzt, dass im Fall von Israel die Samthandschuhe ausgezogen werden. Es kommt dann auch noch dazu, dass das nicht einfach nur beliebige fünfzigtausend Menschen sind auf der Liste. Das sind fünfzigtausend der interessantesten Menschen der Welt, kombiniert mit Daten über ihr Leben! Das ist also eine ganze Story, die Journalisten erzählen können, wenn sie herausfinden können, wer diese Menschen sind.

Eine ehemalige NSO-Sprecherin sagte dem „Guardian“, 9/11 hätte mit Pegasus verhindert werden können.
Das ist ein Witz. Wir wissen, dass die NSA bin Ladens Satellitentelefonnummer hatte. Mindestens seit den 90er Jahren. Damit konnten sie leicht seinen Standort finden. Dass sie 9/11 hätten verhindern können, wenn sie nur diese besonders mächtigen Werkzeuge gehabt hätten, das ist eine komplett irreführende Aussage. Eine klassische NSA-Aussage. Was sie wirklich meinen ist: Wenn wir dieses Tool und eine Zeitmaschine gehabt hätten! Und auch das ist eine Lüge. Während der Snowden-Affäre fanden wir zum Beispiel heraus, dass die NSA die Telefone der Leute kompromittiert hatte, die an dem Bombenanschlag in Mumbai beteiligt waren, bei dem über 300 Menschen getötet wurden. Und zwar bevor der Bombenanschlag stattfand! Und dann gaben sie dem indischen Geheimdienst keinen Tipp, dass sie die Telefone der Terroristen kompromittiert hatten. Warum also haben sie das nicht verhindert? Sie wollten nicht offenlegen, dass sie diese technischen Möglichkeiten haben – und es starben 300 Menschen! Ich war beteiligt, als Pro Publica und die „New York Times“ eine Geschichte darüber gemacht haben. Im Wesentlichen ist meine Schlussfolgerung: Dass die pure Existenz solcher technischen Möglichkeiten solche Dinge verhindern würde, ist eine Lüge. Nur weil die NSA wusste, dass der Anschlag passieren würde, heißt das nicht, dass er auch verhindert wurde. Mumbai hat das bewiesen.

Das macht es schwer den Aussagen der NSA zu trauen.
Man traut ihnen deshalb nicht, weil sie nicht transparent sind und sagen: „Seht her, es gab Zeiten, in denen die Telefone von Leuten kompromittiert wurden, und wir wollten unsere technischen Fähigkeiten nicht offenlegen, also haben wir eine Entscheidung getroffen.“ Das wäre ein Maß an Ehrlichkeit, das die NSA einfach nicht aufbringen kann. Wenn sie das täten, könnte man verstehen was ihre Werte sind und wie ihr Entscheidungsprozess tatsächlich abläuft. Was bedeutet, dass sie manchmal Menschen bei Terroranschlägen sterben lassen, um ihre Fähigkeiten geheim zu halten. Damit unterscheiden sie sich nicht so sehr von den Briten während des Zweiten Weltkriegs – die wussten, dass Coventry bombardiert werden würde. Aber wenn sie zugegeben hätte, dass sie es wußten, hätte die Nazis widerum gewusst, dass deren Krypto-System, wie zum Beispiel das Enigma-System, geknackt wurde. Und so mussten sie die Stadt bombardieren lassen. Das ist mein Verständnis der Geschichte von Coventry. Und es ist im Grunde die gleiche Entscheidungsgrundlage, die man bei dem Bombenanschlag in Mumbai sehen kann.

Kann man nur ohne Smartphone ganz sicher sein?
Wenn Sie Verbrauchergeräte von der Stange wie ein iPhone oder ein Android-Telefon verwenden, sollten Sie bedenken, dass die sehr leicht zu kompromittieren sind und extrem schwer herauszufinden ist, ob Sie kompromittiert wurden. Es ist eine ziemlich beängstigende Welt da draußen. Das eigentliche Problem ist aber, dass Tools wie Pegasus übers Smartphone hinauswachsen werden, je mehr Geräte die Leute im Haus haben. Wissen Sie, die gleiche Art von Malware gibt es auch für Laptops. Wenn man sich ein modernes MacBook anschaut, ist eine interessante Funktion, dass der Deckel das Mikrofon elektronisch ausschaltet, wenn man ihn herunterklappt. Selbst wenn der Computer befallen ist, kann er nicht als Wanze benutzt werden, sobald er geschlossen ist. Das sagt Apple. Es braucht nicht viel Fantasie, um zu überlegen, was auf Smarthome-Assistenten wie Alexa möglich ist.

Geht das auch bei Telefonen?
Man kann das Mikrofon oder andere Geräte abhören. Normalerweise zerlege ich deshalb das Telefon, entferne die Mikrofone und die Lautsprecher. Und wenn ich einen Anruf machen will, stecke ich ein Headset mit externem Mikrofon ein, das habe ich jetzt auch gemacht. Den Anruf den wir gerade führen kann das aber nicht schützen, wenn mein Telefon von irgendeinem verrückten, gut finanzierten Geheimdienst oder auch einer Firma kompromittiert ist. Dann ist die Tatsache, dass ich die Mikrofone entfernt habe egal, denn letztendlich wollen sie die Anrufe abhören. Aber man kann ihnen zumindest den Raumton vorenthalten. Wenn Sie ins Visier von Leuten geraten, die Millionen Dollar für elektronische Kriegsführung ausgeben, sind Sie besser dran, wenn Sie die alten John le Carré-Tricks anwenden: Persönliche Treffen. Nehmen Sie kein Handy mit. Seien Sie vorsichtig mit Ihrer gesamten Kommunikation. Es ist möglich, ohne ein Handy zu leben. Aber es bleibt knifflig. Denn wenn Sie Ihre Telefone abschaffen, sind Sie vielleicht der einzige in Ihrem Dorf, der das tut. Und dann wird stattdessen einfach Ihr Haus verwanzt.

Es ist ein echtes Dilemma.
Jeder muss für sich eine individuelle Einschätzung treffen, worüber er sich Sorgen macht. Sehen Sie sich unseren verwanzten Planeten an: Es gibt Websites wie zum Beispiel buggedplanet.info, die ein Freund von uns betreibt, wo man die Fähigkeiten zur Überwachung in verschiedenen Ländern sehen kann. Doch diese Überwachungs-Landkarte wird irgendwann die ganze Welt zeigen. Jeder Nationalstaat wird irgendwann einen modernen Geheimdienst haben. Er wird über Software zur elektronischen Kriegsführung verfügen, und es wird kostenlose Versionen dieser Tools online geben. Sie müssen also nur ein paar Computer-Nerds bezahlen, um da mitzumachen. Irgendwann wird buchstäblich jedes Land auf der Welt eine Abteilung haben, die sich mit dieser Art von Dingen beschäftigt. Und wenn sie an Ihre iPhone-Nummer oder Ihre iCloud-Kennung rankommen, können sie einfach Ihr Telefon ins Visier nehmen. Und mit null technischem Wissen – einfach die Telefonnummer eintippen, einen Knopf drücken und das Telefon ist eine Wanze! Das ist etwas, wofür man früher eine Menge technisches Geschick brauchte. Jetzt nicht mehr.

Diese Erkenntnis verdanken wir auch dem Pegasus-Projekt.
Die Leute, die damit zu tun haben, scheinen einen wirklich guten Job gemacht zu haben. Gut, es gibt ein paar Spitzfindigkeiten, zum Beispiel, warum die Liste nicht öffentlich ist, was die genaue Quelle ist und wie die Daten aussehen. Aber das, was wirklich zählt, ist, dass sie überprüft haben, dass die Daten authentisch sind. Das ist das Wichtigste. Und es wäre schön, wenn sie einen so transparenten Ansatz wie WikiLeaks verfolgen würden. Ich bin wirklich traurig, dass Julian im Gefängnis sitzt. Er würde wahrscheinlich einen ähnlichen Standpunkt vertreten. Wissen Sie, den Leuten Zugang zu diesen Daten zu geben, würde dem Problem eine ganz andere Dimension geben. Aber davon abgesehen denke ich, dass sie wirklich gute Arbeit geleistet haben und auch weiterhin leisten werden. Und ich denke, dass das technische Team von Amnesty in seiner Arbeit weiter unterstützt werden sollte. Amnesty sollte die besten forensischen Werkzeuge auf dem Planeten haben. Sie sollten ein Programm für Menschenrechtler haben, die ins Visier genommen werden, um sie anrufen zu können und ihre Telefone zu analysieren. Das ist wichtig, um diese Industrie zu verstehen. Das technische Team von Amnesty hat sehr wichtige Arbeit geleistet. Nichtsdestotrotz sollten wir nicht vergessen, dass es Julian Assange war, der mit den Spyfiles-Publikationen die Überwachungsindustrie und deren Einsatz zu politischen Zwecken aufdeckte und diese Art von Recherche in großem Stil begann.

Ist diese Art von Spyware überall illegal?
Es kann in einem Land legal und in einem anderen Land illegal sein kann, diese Werkzeuge zu benutzen. Aber es geht nicht wirklich um legal und illegal. Wenn sie den Präsidenten von Frankreich ins Visier nehmen, dann ist das Spionage. Es ist keine Frage von Terrorismus, der verhindert werden soll. Es ist einfach nur Spionage. Und das bedeutet, dass wir als Journalisten nicht in der Pflicht sind, darüber zu schweigen.

Wer kann Pegasus und Co. einen Riegel vorschieben?
Apple hat hier eine große Verantwortung, genauso wie Google. Diese Firmen haben die Ressourcen und das Know-How, ein ganzes Team von Ingenieuren auf die Lösung des Problems anzusetzen. Dafür gibt es genug Budget, es wäre ein Leichtes für sie. Aber wenn sie das tun, wird es wahrscheinlich damit enden, dass ein NSA-Mitarbeiter oder ein anderer Geheimdienstmitarbeiter ihre Firma infiltriert, um Hintertüren in ihren Code einzubauen. Das ist das Spiel, das im Moment gespielt wird. Das wissen wir aus den Snowden-Akten: CIA, NSA und andere Gruppen schicken Leute in Firmen, um im Auftrag dieser Geheimdienste üble Sachen zu machen. Es geht dabei, wie gesagt, nicht nur um die NSO-Gruppe. Apple könnte einfach ein paar Millionen Dollar an Ingenieurzeit auf dieses Problem ansetzen. Sie würden dabei nicht alle Probleme lösen. Aber sie würden es viel schwieriger und viel teurer machen, die ganze Dynamik der Spionageindustrie wäre betroffen. Aber, wissen Sie, sie werden das nicht tun, weil es nicht wirklich in ihrem Interesse ist. Diese Firmen sind auch auf das Wohlwollen von Regierungen angewiesen, um ihre Produkte zu verkaufen, und verhalten sich entsprechend. iCloud in China zum Beispiel ist komplett einsehbar für die chinesische Regierung. Die Frage ist also, ob die großen Tech-Firmen überall einen guten Job machen, die Daten ihrer Kunden zu schützen, oder ob sie ähnliche zwielichtige Deals wie diesen mit der chinesischen Regierung auch über unsere Daten abschließen. Das ist der Punkt, an dem wir wirklich zusehen müssen, dass der öffentliche Druck zunimmt. Denn so gesehen nutzt die NSO-Gruppe in gewisser Weise nur den Markt aus, den Firmen wie Apple geschaffen haben.

■ Angela Richter ist Regisseurin und Journalistin. Ihr Stück „Assassinate Assange“ von 2012, bei dem auch Jacob Appelbaum mitwirkte, beruht auf Interviews mit dem Whistleblower Julian Assange.

PA/ DPA/I. WAGNER