KULTUR NEU ENTDECKEN

SWR2

SWR2 Wissen

Überwachungstechnik aus Israel – Die Handy-Hacker

Von Benjamin Hammer

Online ab Sonntag, 24. Januar 2021
Redaktion: Gábor Páal
Produktion: SWR 2021

Israels Cyber-Unternehmen knacken selbst verschlüsselte Handy-Kommunikation. Die Firmen gelten als führend in dieser Technik und verkaufen sie weltweit. Sie hilft, Terroranschläge zu vereiteln – aber auch Oppositionelle zu überwachen.

MANUSKRIPT

Musik

Autor:
Auf der Welt sind in diesem Moment mehr als drei Milliarden Smartphones in Gebrauch. Wir Menschen tragen die Geräte fast immer bei uns. Häufig liegen sie sogar neben uns, wenn wir schlafen. Wir telefonieren mit den Smartphones, wir schreiben, spielen, fotografieren und hören. Wir recherchieren, flirten, streiten. Wir teilen sehr viele Informationen mit diesen Geräten.

Das macht Smartphones so wertvoll. Auch für Geheimdienste und Ermittlungsbehörden.

Ein Smartphone zu infiltrieren, ist in technischer Hinsicht eine extrem komplexe Aufgabe. Nur wenige Cyber-Unternehmen auf der Welt bieten dafür Dienstleistungen an. Sie machen das teilweise im Verborgenen, teilweise recht offen. Über die Details ihrer Angebote und ihre Kunden sprechen sie aber grundsätzlich nicht.

Die erfolgreichsten Firmen, die den Lauschangriff aufs Smartphone verkaufen, kommen aus Israel.

Ansage:
Die Handy-Hacker – Überwachungstechnik aus Israel. Von Benjamin Hammer aus dem ARD-Studio Tel Aviv.

Autor:
Wie alle Unternehmen der offensiven Cyber-Branche geben sie an, dass mit ihrer Hilfe Verbrechen bekämpft werden. Dass Ermittlungsbehörden mit ihren Produkten potenzielle Attentäter ausspähen können. Dass damit Leben gerettet werden. All das stimmt.

Aber die Hacking-Tools „Made in Israel“ gelangen auch in Länder, die keine Rechtsstaaten sind. Länder, die Oppositionelle verfolgen, kritische Journalist*innen, Menschenrechtsaktivisten.

Musik

Sprecher:
Omar Radi, 34 Jahre alt. Journalist und Menschenrechtsaktivist aus Marokko. Laut der Organisation Amnesty International wird Radi im Jahr 2019 von marokkanischen Behörden ausspioniert. Dafür, so Amnesty, wird das Smartphone des Marokkaners mit der israelischen Software Pegasus angegriffen.

Sprecherin:
Im Juli 2020 wird Omar Radi in Casablanca festgenommen. Ihm werden Spionage für einen ausländischen Geheimdienst sowie Vergewaltigung vorgeworfen. Radi bestreitet die Vorwürfe. Der Journalist hatte zuvor über Korruption in seinem Land berichtet und die Verflechtungen zwischen Unternehmen und der politischen Elite. Kritisch äußerte er sich auch gegenüber dem marokkanischen Königshaus. In einer

Rangliste der weltweiten Pressefreiheit der Organisation „Reporter ohne Grenzen“ steht Marokko auf Platz 133 von 180 Ländern. In einem Interview mit dem Rechercheverbund „Forbidden Stories“ sagt Omar Radi über die Ermittler:

Sprecher:
„Ich lebe in einem autoritären Polizeistaat. Sie wissen alles über mich. Sie haben alle meine Nachrichten, meine Fotos – mein ganzes Privatleben.“

Sprecherin:
Amnesty International schaut sich das Smartphone von Omar Radi genauer an. Demnach wurde sein mobiler Internetbrowser so umgeleitet, dass Pegasus auf das Smartphone des Marokkaners gelangen konnte. Die marokkanischen Behörden weisen die Spionagevorwürfe zurück. NSO Group – das israelische Unternehmen hinter der Software Pegasus – schreibt damals, man gehe den Hinweisen von Amnesty nach. Details könne man aber aus rechtlichen Gründen nicht nennen.

Atmo:
Telefonklang

Autor:
Spionage war schon immer eine komplizierte Angelegenheit. Bis zur Erfindung von elektronischen Abhöreinrichtungen mussten sich die Geheimdienste fast ausschließlich auf die Arbeit von Informanten verlassen. Später kamen Funkverbindungen und Telefone, die man abhören konnte. Das Internet hat die Arbeit von Ermittlungsbehörden und Nachrichtendiensten revolutioniert. Und Smartphones haben diese Revolution noch einmal auf eine ganz neue Ebene gehoben.

O-Ton Yotam Gutman, darüber Übersetzung:
Als Smartphones immer beliebter wurden, wurden Angriffe auf diese Geräte wirklich wertvoll. Vor etwa 15 Jahren, im Jahr 2007 kam das erste iPhone auf den Markt. Das erste richtige Smartphone. Und es gibt keinen Zweifel, dass ab diesem Moment alle Geheimdienste der Welt versuchten, in diese Smartphones einzudringen und ihre Inhalte auszulesen.

Autor:
Yotam Gutman ist der Vermarktungschef des israelischen Unternehmens Sentinel One. Eine von vielen Cyber-Firmen der selbsternannten Startup-Nation. Doch Sentinel One arbeitet nicht am digitalen Angriff, sondern an der Verteidigung. Die Firma schützt Unternehmen auf der ganzen Welt vor Hacker-Angriffen. Gutman schätzt, dass es in Israel 300 Cyber-Unternehmen gibt, die sich auf Abwehr spezialisiert haben. Etwa 15 Firmen stehen auf der anderen, offensiven Seite: Sie programmieren Software oder stellen Hardware her, die Cyber-Angriffe ermöglicht. Dass das kleine Israel in der Cyber-Branche weltweit führend ist: kein Zufall.

O-Ton Yotam Gutman, darüber Übersetzung:
Zunächst ist es eine Frage der Notwendigkeit: In unserer Konfliktregion mussten wir schlicht solche Instrumente entwickeln, um mit den Geheimdiensten die Oberhand zu gewinnen. Hinzu kommt unser gutes Bildungssystem, mit guten Universitäten, die Talente für die Branche hervorbringen. Und dann ist da noch die israelische Armee.

In den Cyber-Einheiten lernen Soldaten in etwa vier Jahren Dinge, für die Menschen in anderen Ländern zehn Jahre brauchen. In diesen Einheiten laufen die Dinge quasi auf Steroiden.

Autor:
Wer die Ausbildung in einer Cyber-Elite-Einheit der israelischen Armee durchlaufen hat, kann sich danach einen Job aussuchen. Einstiegsgehalt: umgerechnet bis zu 25.000 Euro im Monat. Yotam Gutman wählte einen anderen Weg in die Branche. Er ging zur Marine und studierte Geschichte. Der Israeli entschied sich später bewusst für eine Karriere in der Cyber-Verteidigung. Das war nicht immer so. Früher arbeitete er auch mal für ein Unternehmen der sogenannten Cyber-Intelligence-Branche.

O-Ton Yotam Gutman, darüber Übersetzung:
Wir arbeiteten dort an Informationsgewinnung. Im Dark Web und anderen Bereichen. Wir haben zum Beispiel für Banken gearbeitet, die wissen wollten, wer sie angreifen will. Damals wurden wir immer wieder von staatlichen Behörden aus dem Ausland kontaktiert. Die fragten: Können wir Eure Dienste nutzen? Diese potenziellen Kunden sprachen nicht von Spionage. Sie nannten das Überwachung. Da ging es um eine bestimmte Bevölkerungsgruppe. Man wolle wissen, ob die Terroranschläge plane und so weiter. Da dachte ich: Okay, vielleicht ist diese Anfrage legitim. Aber was ist, wenn sie danach die Opposition aushorchen wollen? Oder Journalisten? Und ich merkte: Sobald Du diese Behörden mit den Fähigkeiten ausstattest, können sie sie gegen jeden einsetzen.

Autor:
Unschuldige Menschen könnten ausspioniert werden, sagt Gutman. Als er darüber nachgedacht habe, habe er das Unternehmen verlassen.

Musik

Sprecher:
Ahmed Mansoor. Blogger, Dichter und Menschenrechtsaktivist aus den Vereinigten Arabischen Emiraten. 2011 wird Mansoor festgenommen, weil er die Herrscher der Emirate beleidigt habe. Er kommt im gleichen Jahr frei. 2017 kommt er erneut in Haft. Ein Gericht verurteilt ihn später zu einer Gefängnisstrafe von zehn Jahren. In Social-Media-Beiträgen habe er Unwahrheiten verbreitet sowie der nationalen Einheit geschadet.

Sprecherin:
Ahmed Mansoor wird laut Medienberichten sowie nach Angaben der Organisation Citizen Lab seit Jahren von Ermittlern der Vereinigten Arabischen Emirate überwacht. 2011 soll es einen Angriffsversuch mit Software des deutschen Unternehmens FinFisher gegeben haben. 2012 folgte laut den Berichten ein digitaler Angriff der Firma Hacking Team aus Italien. Die Ermittler der Emirate müssen großes Interesse an den Aktivitäten Mansoors gehabt haben.

Sprecher:
Am 10. August 2016, um 9:38 Uhr Ortszeit erhält Ahmed Mansoor eine SMS-Nachricht auf sein Smartphone. Dort steht:

Sprecherin:
Neue Geheimnisse über die Folterung von Emiratis in staatlichen Gefängnissen.

Sprecher:
Unter dem Text steht ein Link. Aber Ahmed Mansoor ist skeptisch und klickt nicht drauf. Stattdessen schickt der den Link – der auf eine etwas kryptische Adresse führen soll – an die Organisation Citizen Lab in Kanada. Citizen Lab klickt anschließend bewusst und mit einem fabrikneuen Smartphone ohne Daten auf den Link. Das Smartphone, so Citizen Lab, wird danach mit der Spionagesoftware Pegasus von der NSO Group aus Israel infiziert.

Sprecher:
Ahmed Mansoor befindet sich weiterhin in Haft. Sein Gesundheitszustand soll schlecht sein. Human Rights Watch, Amnesty International und das Europäische Parlament fordern seine sofortige Freilassung.

Atmo:
Telefonklang

Autor:
Offensive Cyber-Unternehmen gibt es in mehreren Ländern der Welt. In den USA zum Beispiel, in Italien und auch in Deutschland. Der Export digitaler Lauschangriffe ist also keine rein israelische Spezialität.

Dennoch fällt eine Sache auf, wenn man sich die Branche anschaut: Werden Details über die Aktivitäten der kommerziellen Hacker bekannt, geht es häufig um Unternehmen aus Israel.

Expertinnen und Experten, die kritisch auf die Branche schauen, bestreiten, dass sie sich auf Israel eingeschossen haben. Die meisten Hinweise zu möglichem Missbrauch der Hacking-Software kämen aktuell nun einmal zu Firmen aus Israel, heißt es zum Beispiel von der kanadischen Forschungs-Organisation Citizen Lab der Universität von Toronto.

Ein Mann, der die Branche gut kennt, sagt: Was die Israelis machen, sei sehr viel besser als die Arbeit der Firmen aus anderen Ländern. Dies werde einem jede Ermittlungseinheit auf der Welt bestätigen.

Zwei israelische Unternehmen, die Hacking-Technologien verkaufen, sind besonders bekannt. Die NSO Group und Cellebrite. Beide werben auf ihren Homepages damit, dass ihre Produkte die Welt besser und sicherer machen. Bei NSO heißt es:

Sprecherin:
NSO schafft Technologien, die Regierungsbehörden dabei hilft, Terrorismus und Verbrechen zu bekämpfen und auf der ganzen Welt tausende Leben zu retten.

Autor:
NSO ist vor allem für Pegasus bekannt. Die Software wird auf das Smartphone einer Zielperson geschleust. Früher geschah das vor allem über SMS-Nachrichten, die einen Link enthielten. So wie laut Citizen Lab beim Blogger Ahmed Mansoor aus den

Emiraten. Klickten die Opfer auf den Link, wurde Pegasus auf dem Gerät installiert. Doch mittlerweile kennen viele diese Masche. Deshalb kann Pegasus auch ohne das Zutun der Zielpersonen auf dem Gerät landen, sagen Insider. Wie von Geisterhand.

Möglich werden die Angriffe durch Lücken in den Betriebssystemen iOS und Android, die die Hersteller nicht kennen. Auch die Netzbetreiber spielen häufig eine Rolle.

Dank Pegasus haben Ermittler praktisch vollen Zugriff auf die Geräte. Können Nachrichten lesen, sich Fotos anschauen. Sogar Fotos machen und das Mikrofon einschalten, berichten Insider.

Die zweite bekannte offensive Cyber-Firma aus Israel heißt Cellebrite. Bei ihrem bekanntesten Produkt wird das Smartphone – anders als bei NSO – nicht aus der Ferne gehackt. Es muss sich in den Händen der Ermittlungsbehörden oder Geheimdienste befinden.

Musik

Sprecher:
Sayed Farook, US-Amerikaner. Farook arbeitet als Sachverständiger für Lebensmittelsicherheit für einen Landkreis in Kalifornien. Er ist ein gläubiger Muslim, der sich nach Einschätzung des FBI radikalisiert hat.

Sprecherin:
Am 2. Dezember 2015 betreten Farook und dessen Ehefrau eine Einrichtung für Menschen mit Behinderung in San Bernadino, Kalifornien. Dort findet gerade eine Weihnachtsfeier statt. Die beiden Attentäter tragen Sturmhauben und schwarze Kleidung. Mit Gewehren eröffnen sie das Feuer. 14 Menschen werden getötet. Farook und dessen Ehefrau fliehen. Bei einem späteren Schusswechsel mit der Polizei werden sie getötet.

Sprecher:
Die Ermittler suchen anschließend dringend nach Hinweisen auf die Motive der Täter. Dafür wollen sie das iPhone 5C von Sayed Farook entsperren. Doch sie scheitern. Zumindest behaupten sie das. Apple, der Hersteller des iPhones, weigert sich, die Sperrung über einen technischen Umweg zu umgehen. Dies verstoße gegen die Firmenpolitik. Der Streit zieht sich über Wochen hin und beschäftigt auch Gerichte. Doch Apple bleibt hart. Etwa vier Monate nach dem Attentat – im Frühjahr 2016 - teilt das US-Justizministerium mit, Zugriff auf das Smartphone von Farouk erlangt zu haben.

Sprecherin:
Laut einem Bericht des US-Senders CBS finden die Ermittler auf dem iPhone des Attentäters keine bedeutsamen Informationen. Die Folgen des Hacks sind dennoch gewaltig: Es wird öffentlich, dass es möglich ist, die verschlüsselten Daten eines iPhones auszulesen. Auch gegen den Willen des Herstellers. Die israelische Zeitung Yedioth Acharonot nennt damals den mutmaßlichen Namen der Firma, die dem FBI geholfen hat: Cellebrite aus Israel. Das Unternehmen hat dies nie bestätigt. Doch heute ist es kein Geheimnis mehr, dass Cellebrite in der Lage ist, Smartphones zu hacken.

Atmo:
Telefonklang

Autor:
Mit wem die israelischen Cyber-Unternehmen zusammenarbeiten, bleibt normalerweise geheim. Jede Behörde weltweit, jeder Nachrichtendienst muss einen Geheimhaltungsvertrag unterschreiben noch bevor überhaupt Vertragsverhandlungen geführt werden. Auch die israelischen Cyber-Firmen geben sich eher zugeknöpft. Die NSO Group ermöglichte für diese Sendung ein Hintergrundgespräch. Aus dem jedoch unter keinen Umständen zitiert werden darf. Deshalb kommt an dieser Stelle David ins Spiel.

Sprecher (David):
Ich heiße gar nicht David. Aber meine wahre Identität muss geheim bleiben. Ich habe jahrelang für eine israelische IT-Firma aus dem Offensivbereich gearbeitet.

Autor:
Was David genau gemacht hat, darf an dieser Stelle nicht berichtet werden. David hat jedoch einer der etwa 15 offensiven israelischen Hacking-Firmen dabei geholfen, Zielpersonen digital auszuspähen.

Sprecher (David):
Ich habe Dinge gemacht, die haben viele Menschen auf diesem Planeten nicht gemacht. Die Leute kannst Du an einer Hand abzählen. Und ja: Da gehöre ich wohl dazu.

Autor:
David machte seinen Job aus Überzeugung. Er wusste, dass die Produkte seiner Firma auch dafür eingesetzt werden können Oppositionelle zu verfolgen. Doch für ihn überwog, dass mit seiner Hilfe Verbrechen verhindert wurden.

Sprecher (David):
Ich habe mit meiner Arbeit Ermittlungsbehörden und Geheimdienste unterstützt. Da ging es vor allem um die Bekämpfung von Kriminalität. Um den Kampf gegen Kinderpornographie. Gegen den Terrorismus, organisierte Kriminalität, Menschenhandel. Und so weiter. Das war immer der Grund, warum ich mitgemacht habe. Mein Antrieb.

Autor:
David sagt: Keine der israelischen Firmen verkaufe ihre Produkte, damit gezielt Menschenrechtsverbrechen begangen werden. In den Verträgen, die mit den Ermittlungsbehörden abgeschlossen würden, stehe klipp und klar, dass die Produkte nicht missbraucht werden dürfen. Aber natürlich würden manche Länder die Israelis nicht informieren, wenn sie krumme Dinger machen. Und die Israelis schauten auch nicht immer gründlich hin. Auch, weil das Geschäft sehr lukrativ sei:

Sprecher (David):
Weißt Du, was diese Firmen verdienen? Kennst Du den Marktwert von denen? Was glaubst Du, was die Firmen wert sind? Und glaubst Du, die Unternehmenschefs

lassen sich davon nicht beeindrucken? Die müssen abliefern gegenüber den Investoren. Die wollen Zahlen sehen. Und Moral interessiert die Investoren gar nicht.

Autor:
Die NSO Group wurde im Jahr 2017 so richtig bekannt. Damals wurde berichtet, wie staatliche mexikanische Ermittlungsbehörden Anwälte, Journalistinnen und Aktivisten ausspähten. Angeblich mit der Software Pegasus.

Enthüllt wurde auch das von dem Think Tank Citizen Lab der Universität von Toronto. Die Forscherinnen und Forscher beschäftigen sich dort mit den Zusammenhängen von IT, Kommunikation und Menschenrechten. Zum Team gehört auch der promovierte Informatiker Bill Marczak.

O-Ton Bill Marczak, darüber Übersetzung:
Nehmen wir an, dass sich die Firmen bestimmte Länder genauer anschauen, bevor sie ihre Produkte dorthin verkaufen. Mexiko, die Vereinigten Arabischen Emirate oder Saudi-Arabien zum Beispiel. Dann ist es doch eigentlich sehr einfach, vorab Nachweise zu finden, dass es in diesen Ländern ernste Probleme mit der Rechtstaatlichkeit und den Menschenrechten gibt. Wenn nun in diese Länder auch noch sehr mächtige Spionage-Software verkauft wird, wird das die Lage nicht unbedingt verbessern.

Autor:
Aus Sicht des Informatikers Marczak entbehrt es nicht einer gewissen Ironie, dass ein großer Teil der exportierten Hacking-Werkzeuge aus Israel stammt. Aus einer gestandenen Demokratie also.

O-Ton Bill Marczak, darüber Übersetzung:
Mich besorgt, dass Demokratien auf der ganzen Welt unter Druck sind. Länder, in denen es danach aussah, dass sie demokratischer werden, zeigen nun verstärkt autoritäre Tendenzen. Und ich denke, dass Länder, die demokratisch sind, diese Entwicklung anerkennen und danach handeln müssen. Diese Demokratien dürfen keine Werkzeuge verkaufen, die autoritäre Bestrebungen stärken.

Musik

Sprecher:
Joshua Wong, Aktivist und Politiker aus Hongkong. 24 Jahre alt. 2014 ist Wong eines der bekanntesten Gesichter der Studierenden-Proteste, die weltweit unter dem Namen „Regenschirm-Revolution“ bekannt wurden. Er gründet später die pro-demokratische Partei Demosisto. Die Partei löst sich im Sommer 2020 auf, nachdem Chinas Staats- und Parteiführung ein sogenanntes Sicherheitsgesetz für Hongkong beschlossen hatte. Dieses Gesetz hat die völkerrechtlich zugesicherte Autonomie Hongkongs de facto außer Kraft gesetzt. So werden in Hongkong Rechtsstaatlichkeit und Meinungsfreiheit in vielen Bereichen abgeschafft.

Sprecherin:
Ende 2020 wird Joshua Wong zu einer Gefängnisstrafe von einem Jahr und einem Monat verurteilt. Er habe eine unerlaubte Protest-Kundgebung organisiert und andere dazu aufgerufen, daran teilzunehmen.

Sprecher:
Am 17. Juli 2020 wendet sich ein Mitstreiter von Wong, Nathan Law, in einem Beitrag auf Facebook an die israelische Firma Cellebrite. „Hört auf damit, für China Smartphones zu hacken“, schreibt er. Cellebrite helfe der Polizei von Hongkong seit langem, die Smartphones von Aktivistinnen und Aktivisten auszulesen. Das iPhone von Joshua Wong sowie die Geräte von 4.000 weiteren Festgenommenen seien innerhalb eines Jahres mit der Technologie von Cellebrite geknackt worden.

Sprecherin:
Zu den konkreten Vorwürfen äußert sich Cellebrite nicht. Das israelische Unternehmen teilt jedoch im Herbst 2020 mit: Ab sofort verkaufe man keine Produkte mehr nach Hongkong und Festlandchina. Die Begründung fällt eher knapp aus. Cellebrite nennt „veränderte Richtlinien“ in den USA. Die US-Regierung unter Donald Trump hatte sich zuvor immer wieder an die Seite der Aktivisten in Hongkong gestellt.

Atmo:
Telefonklang

Autor:
Wenn man mit Vertreterinnen und Vertretern der offensiven Cyber-Branche spricht, wird es manchmal emotional. Sie fühlen sich zu Unrecht an den Pranger gestellt. Denn sie würden nur die Technologien liefern. Für den Einsatz seien die Ermittler verantwortlich. Aus ihrer Sicht wird viel zu viel über den angeblichen Missbrauch ihrer Software durch Diktaturen berichtet. Und viel zu wenig über den rechtmäßigen Einsatz in Demokratien. Wo die Ermittler nur mit einem Gerichtsbeschluss einen digitalen Spionage-Angriff starten dürfen.

Die Befürworter der Branche verweisen darauf, dass die Welt ohne ihre Produkte ein gewaltiges Problem hätte: Denn die meisten Kommunikation auf Smartphones ist mittlerweile verschlüsselt. Nur mit den digitalen Werkzeugen – so das Argument könnten Ermittler herausfinden, was Kriminelle vorhaben.

Tehilla Shwartz Altshuler ist nicht per se gegen die Hacking-Tools. Die Juristin forscht am israelischen Institut für Demokratie in Jerusalem.

O-Ton Tehilla Shwartz Altshuler, darüber Übersetzung:
Wissen Sie, in den vergangenen 100 Jahren haben Gerichte in allen Demokratien das klar definiert: Diese Instrumente dürfen eingesetzt werden, wenn unmittelbare Gefahr besteht. Wenn wir über Terroristen reden, über tickende Zeitbomben, über Gefahren für die nationale Sicherheit, dann würde ich definitiv jede verfügbare Technologie einsetzen, um Leben zu retten.

Autor:
Kritisch sieht Tehilla Shwartz Altshuler dagegen den Einsatz israelischer Überwachungssoftware gegen Journalisten oder Menschenrechtler in Ländern wie den Vereinigten Arabischen Emiraten oder Mexiko, wie es das Citizen Lab behauptet. Eine zentrale Rolle spiele dabei das israelische Verteidigungsministerium, das den Export von Pegasus und Co überwacht.

O-Ton Tehilla Shwartz Altshuler, darüber Übersetzung:
Manchmal erlaubt die israelische Regierung den Export von solchen Technologien in Länder, mit denen Israel geostrategische Interessen verbindet. So sagt die Regierung zum Beispiel: Bitte verkauft diese Technologie nach Ägypten oder in andere arabische Staaten. Das sind keine Demokratien. Aber wir haben ein Interesse daran, dass in diesen Regimen Stabilität herrscht.

Autor:
Ein Argument, dass auch bei Waffenexporten aus europäischen Ländern kommt. Zum Beispiel nach Saudi-Arabien. Israel kämpfte seit der Staatsgründung mehrere Kriege mit arabischen Staaten. Ist im Nahen Osten in Teilen isoliert. Lange gab es nur Friedensabkommen mit den Nachbarländern Ägypten und Jordanien. Erst in den vergangenen Monaten wurden Abkommen mit den Vereinigten Arabischen Emiraten, Bahrain, dem Sudan und Marokko auf den Weg gebracht. Lange bevor solche Beziehungen sichtbar werden, kooperieren die Geheimdienste miteinander. Mutmaßlich auch mit Technologietransfer.

Dass Geostrategie alles überwiegt, weist das israelische Verteidigungsministerium zurück. Die Entscheidung, ob ein Cyber-Produkt exportiert werden dürfe, hänge von verschiedenen Faktoren ab. Darunter die Frage von Menschenrechten. Ein wichtiger Faktor, sagt die Juristin Shwartz Altshuler, sei jedoch, dass die israelische Armee und die Geheimdienste die Technologien selbst einsetzten. Das Verteidigungsministerium sei damit gleichzeitig Auftraggeber und Kontrollbehörde. Eine schwierige Konstellation. Und es gebe ein weiteres Problem, sagt die Frau vom Demokratie-Institut. Dem israelischen Verteidigungsministerium fehle es schlicht an Kenntnissen, um die Cyber-Unternehmen und ihre extrem komplizierten Programmiercodes überprüfen zu können.

O-Ton Tehilla Shwartz Altshuler, darüber Übersetzung:
Ich hatte mal ein sehr interessantes Gespräch mit dem Chef von einer dieser Überwachungsfirmen. Und er sagte mir: Du machst Dir keine Vorstellungen. Ich musste der Kontrollbehörde beibringen, was Überwachungssysteme sind. Und welchen Schaden sie anrichten können. Ich musste der Kontrollbehörde beibringen, wie sie mich kontrolliert.

Autor:
Tehilla Shwartz Altshuler hat einen offenen Brief veröffentlicht. Sie wendet sich an die junge Israelis, die ihren Wehrdienst in einer der Cyber-Elite-Einheiten der Armee beenden. Und sich entscheiden müssen, für wen sie arbeiten.

O-Ton Tehilla Shwartz Altshuler, darüber Übersetzung:
Ich schrieb ihnen: „Ihr seid gute Leute, der Stolz israelischer Mütter. Wir erwarten von Euch, dass Ihr Eure Talente dafür nutzt, die Welt zu reparieren. Gutes zu tun. Fangt bei Social-Media-Firmen an, arbeitet an autonomen Fahrzeugen, arbeitet an klimafreundlichen Technologien. Ihr müsst nicht für Firmen arbeiten, deren Produkte der Welt schaden und Diktaturen stärken."

Autor:

Eine Sichtweise, die die NSO Group zurückweist. Das Unternehmen, heißt es in einer schriftlichen Stellungnahme, sei nur aus einem Grund geschaffen worden. Ermittlungsbehörden und Nachrichtendiensten zu helfen, Leben zu retten und Sicherheit zu gewährleisten. NSO betreibt nach eigener Aussage ein internes Prüfgremium. Das soll dafür sorgen, dass die Hacking-Software Pegasus nur rechtstaatlich gebraucht und nicht missbraucht wird.

Musik

Atmo:
Tippen

Autor:
NSO verspricht, ein Dilemma zu lösen, vor dem die Welt steht: Die Firma will in Zeiten verschlüsselter Daten Verbrechen bekämpfen, ohne dass die mächtige Spionage-Software von Staaten missbraucht wird. Das klingt gut. Aber die Kritikerinnen und Kritiker von Firmen wie NSO sagen, dass die Realität diesem Versprechen nicht standhält.

Ein hochrangiger Manager des US-Softwarekonzerns Microsoft wurde vor wenigen Wochen deutlich. Er nannte die Mitarbeiterinnen und Mitarbeiter der NSO Group „Cyber-Söldner“. Das bekannteste Produkt von NSO – Pegasus – nannte er nicht Software. Der Microsoft-Manager benutze das Wort „Waffe“.

*****