Warum wird Israel nicht für das Ausspionieren von Journalisten zur Rechenschaft gezogen?

Ali Abunimah, electronicintifada.net, 19. .07.21

Die von der israelischen Firma *NSO Group* hergestellte Spionagesoftware wurde in weit größerem Umfang als bisher bekannt gegen Journalisten und Menschenrechtsaktivisten in aller Welt eingesetzt.

Dies wirft die Frage auf, warum Israel, der staatliche Akteur, ohne den die NSO Group nicht existieren würde und nicht operieren könnte, nicht zur Rechenschaft gezogen wird.

Vergangenes Jahr wies ein israelisches Gericht einen Versuch von *Amnesty International* zurück, die israelische Regierung zu zwingen, die Exportlizenz der *NSO Group* zu widerrufen.

Das Ausmaß der Spionage ist dank einer groß angelegten Untersuchung ans Licht gekom-men, die von dem globalen Berichterstattungs-konsortium *Forbidden Stories* und der Menschenrechtsgruppe *Amnesty Internatio-nal* geleitet wurde.

„Eine beispiellose Veröffentlichung von mehr als 50.000 Telefonnummern, die von den Kunden des israelischen Unternehmens *NSO Group* zur Überwachung ausgewählt wurden, zeigt, wie diese Technologie seit Jahren systematisch missbraucht wird", so *Forbidden Stories*.

Die Spyware mit dem Namen *Pegasus* kann aus der Ferne auf dem Smartphone einer Zielperson installiert werden, ohne dass diese eine Aktion wie das Anklicken eines Links oder die Annahme eines Anrufs ausführen muss.

„Einmal installiert, ermöglicht es den Kunden, die vollständige Kontrolle über das Gerät zu übernehmen, einschließlich des Zugriffs auf Nachrichten von verschlüsselten Messaging-Apps wie *WhatsApp* und *Signal* und des Einschaltens des Mikrofons und der Kamera“, so *Forbidden Stories*.

Pegasus wird angeblich nur an Regierungen verkauft, die es für legitime Strafverfolgungszwecke einsetzen.

Doch laut *Forbidden Stories* wurde diese Spionagesoftware in großem Umfang missbraucht, entgegen den langjährigen Behauptungen der *NSO Group*, die auch in einem kürzlich veröffentlichten Transparenzbericht enthalten sind. Zu den für *Pegasus* ausgewählten Zielpersonen gehören mindestens 180 Journalisten in Ländern wie Indien, Mexiko, Ungarn, Marokko, Frankreich, Spanien, Großbritannien, Ägypten, dem Libanon und den Vereinigten Arabischen Emiraten.

Weitere potenzielle Zielpersonen sind Menschenrechtsverteidiger, Akademiker, Rechtsanwälte, Gewerkschafter, Ärzte, Politiker und sogar Staatschefs.

Forbidden Stories sagt, dass es unmöglich ist, zu wissen, ob eine der 50.000 Telefonnummern auf der Liste, die es erhalten hat, erfolgreich angegriffen wurde, solange nicht das konkrete Gerät untersucht wird, das mit einer Nummer verbunden ist.

Die *NSO-Group* soll noch in diesem Jahr an einer Pariser Ausstellung zum Thema „Innere Sicherheit" teilnehmen. Die Milipol-Ausstellung wird von der französischen Regierung gesponsert.

Das Sicherheitslabor von *Amnesty International* nahm forensische Untersuchungen an den Telefonen von mehr als einem Dutzend Journalisten und insgesamt an fast 70 Telefonen vor. Sie „deckten erfolgreiche Infektionen durch eine Sicherheitslücke in iPhones auf, auch aus diesem Monat", so *Forbidden Stories*.

„Diese Nachforschungen haben weit verbreitete, anhaltende und fortgesetzte ungesetzliche Überwachung und Menschenrechtsverletzungen ergeben, die mit Hilfe der Spionagesoftware Pegasus der NSO Group begangen wurden", so Amnesty.

Verbindung zum Khashoggi-Mord

Vor den jüngsten Enthüllungen wurde der Einsatz von *Pegasus* bereits mit dem Mord an dem Washington-Post-Kolumnisten Jamal Khashoggi im saudi-arabischen Konsulat in Istanbul im Jahr 2018 in Verbindung gebracht.

Nach dem Mord an Khashoggi stellte die *NSO Group* zur Schadensbegrenzung unter anderem die gut vernetzten ehemaligen Beamten der Obama-Regierung Juliette Kayyem ein, die im US-Ministerium für Innere Sicherheit arbeitete, und Daniel Shapiro, der als US-Botschafter in Israel tätig war.

Die neuen Untersuchungen zeigen, dass Rodney Dixon, ein prominenter Menschenrechtsanwalt mit Sitz in Großbritannien, im Jahr 2019 von *Pegasus* ins Visier genommen wurde, die Untersuchung seines Geräts jedoch keine erfolgreiche Infektion ergab.

Dixon vertrat einen Briten, der in den Vereinigten Arabischen Emiraten inhaftiert ist, einer eng mit Israel verbündeten Diktatur am Golf, von der seit langem bekannt ist, dass sie *Pegasus* nutzt. Dixon hat auch Hatice Cengiz vertreten, die mit Khashoggi verlobt war. Eine gerichtsmedizinische Untersuchung ergab, dass Cengiz' eigenes Telefon angegriffen und tatsächlich infiziert war.

Dixon ist auch Anwalt der Opfer des israelischen Angriffs auf das Schiff Mavi Marmara im Jahr 2010, die versuchen, vor dem Internationalen Strafgerichtshof Recht zu bekommen.

Israels Rolle heruntergespielt

Die neuen Enthüllungen über die *NSO Group* finden ein breites Echo in den Medien, wobei die Rolle Israels, insbesondere die der Regierung, von den wichtigsten englischsprachigen Mitgliedern des Konsortiums *Forbidden Stories* heruntergespielt wird. Der Leitartikel des *Guardian* zu diesem Thema enthält keinen Hinweis auf Israel in der Überschrift und nur eine Erwähnung im Artikel selbst, in der die *NSO Group* als israelisches Unternehmen beschrieben wird.

Die *Washington Post* schneidet mit der Schlagzeile „Mit privater israelischer Spionagesoftware weltweit Handys von Journalisten und Aktivisten gehackt“ etwas besser ab.

Aber diese Betonung auf „privat“ verschleiert, dass die israelische Regierung eine zentrale Rolle bei der Existenz und den laufenden unlauteren Aktivitäten der *NSO Group* spielt.

In 35 Absätzen des Post-Artikels versteckt findet sich das Zugeständnis, dass „*Pegasus* vor einem Jahrzehnt von israelischen Ex-Cyberspionen mit von der Regierung erworbenen Fähigkeiten entwickelt wurde“.

„Das israelische Verteidigungsministerium muss jede Lizenz an eine Regierung, die es kaufen will, genehmigen, so frühere Aussagen des NSO", fügt die Post hinzu.

Die Rolle der israelischen Regierung bei der Erteilung von Lizenzen für die Verkäufe der *NSO Group* scheint nicht nur ein passiver Prozess der Erteilung von Genehmigungen zu sein. Vielmehr sieht Israel diese Firmen als Erweiterung seines Einflussbereichs, da es Beziehungen zu Regierungen in der gesamten Region pflegt.

Unter Berufung auf einen israelischen Beamten und Quellen aus dem Unternehmen berichtete die *New York Times* diese Woche, dass die israelische Regierung „NSO und zwei weitere Unternehmen ermutigt hat, weiterhin mit Saudi-Arabien zusammenzuarbeiten, und einem vierten Unternehmen eine neue Lizenz für eine ähnliche Tätigkeit erteilt hat, wobei sie sich über alle Bedenken wegen Menschenrechtsverletzungen hinweggesetzte".

Vergangenes Jahr wies ein israelisches Gericht einen Versuch von *Amnesty International* zurück, die israelische Regierung zu zwingen, die Exportlizenz der *NSO Group* zu widerrufen.

Amnesty sprach von einem „schändlichen Urteil“ und einem „grausamen Schlag für Menschen in aller Welt, die durch den Verkauf von Produkten der NSO Group an notorische Menschenrechtsverletzer gefährdet sind“.

Die New York Times - die nicht Teil des Forbidden Stories-Konsortiums war - hebt hervor, dass die jüngsten Enthüllungen „die Besorgnis verstärken könnten, dass die israelische Regierung staatlichen Missbrauch begünstigt hat, indem sie NSO eine Exportlizenz für den Verkauf von Software an Länder erteilte, die diese zur Unterdrückung von Dissidenten einsetzen".

Die New York Times berichtete bereits früher, dass Pegasus weitgehend von Veteranen der Einheit 8200 entwickelt wurde.

Die Einheit 8200 ist die Cyberwar-Abteilung des israelischen Militärs, die direkt für die massive Überwachung und Menschenrechtsverletzungen an Palästinensern verantwortlich ist, die unter israelischer militärischer Besatzung leben.

Zweifellos wurden die Spionagetechnologien, die heute weltweit gegen Menschenrechtsaktivisten eingesetzt werden, an einer gefangen gehaltenen palästinensischen Bevölkerung entwickelt und getestet.

Ablenkung der Aufmerksamkeit in Richtung China

Das unverhältnismäßige Schweigen über die direkte und unbestrittene Rolle der israelischen Regierung bei den üblen Aktivitäten der NSO Group steht im Gegensatz zur jüngsten Kampagne der westlichen Regierungen gegen China.

Am Montag beschuldigte die Regierung Biden die chinesische Regierung, die E-Mail-Systeme von Microsoft zu hacken, die von Unternehmen und Regierungsstellen in aller Welt genutzt werden.

In einer Erklärung des Weißen Hauses wurden diese bösartigen Cyberangriffe „mit einem hohen Maß an Vertrauen“ der chinesischen Regierung zugeschrieben - ein Geheimdienstcode dafür, dass die USA keine handfesten Beweise haben.

Auch Kanada schloss sich den Anschuldigungen der USA gegen chinesische „staatlich unterstützte Akteure“ an, doch eine Erklärung des Außenministeriums in Ottawa ist mit schwammigen Worten gespickt – „Kanada ist zuversichtlich …“. „Kanada hält es für sehr wahrscheinlich …“ - was darauf hindeutet, dass es sich um Anschuldigungen und nicht um unumstößliche Fakten handelt.

Dieser Mangel an Beweisen wird durch die Erklärung der Europäischen Union bestätigt, die sich noch vager dazu äußert, wer für die angeblichen Microsoft-Hacks verantwortlich sein könnte.

Im Gegensatz zu ihren amerikanischen und kanadischen Verbündeten beschuldigt die EU nicht direkt China oder chinesische „staatlich unterstützte Akteure“, sondern behauptet lediglich, dass „die EU und ihre Mitgliedstaaten davon ausgehen, dass diese bösartigen Cyber-Aktivitäten vom chinesischen Hoheitsgebiet aus unternommen wurden“.

EU zuckt mit den Schultern

In Anbetracht der Tatsache, dass Menschenrechtsverteidiger und Journalisten in mehreren EU-Mitgliedsstaaten ins Visier von Pegasus *geraten* sind oder dafür ausgewählt wurden, fragte T*he Electronic Intifada* den außenpolitischen Sprecher der EU, ob die EU über bösartige Cyber-Aktivitäten besorgt sei, die von Israel ausgehen, einem Staat, mit dem er eng verbündet ist.

In der 187 Wörter umfassenden Antwort des EU-Sprechers für Außen- und Sicherheitspolitik wurde Israel mit keinem Wort erwähnt.

„Angelegenheiten der nationalen Nachrichtendienste fallen in die nationale Zuständigkeit, und es ist Sache der nationalen Behörden, ihre eigenen Dienste zu beaufsichtigen“, erklärte die EU.

Das ist ein klarer Hinweis darauf, dass die EU nicht die Absicht hat, zu untersuchen, wie der ungarische Ministerpräsident Viktor Orban Berichten zufolge die israelische Spionagesoftware gegen Kritiker und Journalisten in einem EU-Mitgliedstaat einsetzt.

„Überwachungstechnologien können, wenn sie auf ethische Weise und im Einklang mit dem Gesetz eingesetzt werden, wirksame Instrumente zur Strafverfolgung sein“, fügte die EU hinzu und befürwortete damit offensichtlich die fragliche *Malware* [Schadsoftware].

Die EU räumte jedoch ein, dass es „immer mehr Berichte über Missbrauch und Menschenrechtsverletzungen aufgrund des Einsatzes digitaler Überwachungsinstrumente" gebe, vor allem gegen Journalisten und Menschenrechtsverteidiger.

Die EU forderte die Staaten auf, „Gesetze und Schutzmaßnahmen einzuführen, um die Menschen vor unrechtmäßiger oder unnötiger Überwachung, einschließlich willkürlicher oder massenhafter Überwachung, zu schützen“.

Sie kündigte außerdem an, „alle unsere politischen Instrumente, einschließlich der Menschenrechtsdialoge, zu nutzen, um die Besorgnis über den unrechtmäßigen Einsatz von Überwachungstechnologien weiter zu schüren“.

Das ist ein zahnloses Versprechen angesichts des völligen Schweigens der EU zu Israel, einem wichtigen staatlichen Akteur, der solche Missbräuche in der ganzen Welt und in der EU selbst ermöglicht.

Die *NSO-Group* soll noch in diesem Jahr an einer Pariser Ausstellung zum Thema „Innere Sicherheit“ teilnehmen. Die Milipol-Ausstellung wird von der französischen Regierung gesponsert.

Übersetzung: Pako – palaestinakomitee-stuttgart.de

Quelle: https://electronicintifada.net/blogs/ali-abunimah/why-isnt-israel-held-accountable-spying-journalists