Mittwoch, der 19. April, ist der weltweite Aktionstag gegen Spyware. Zivilgesellschaftliche Gruppen, Menschenrechtsorganisationen und einzelne Aktivistinnen und Aktivisten aus der ganzen Welt beteiligen sich an der Forderung, die Technologie zu verbieten, die es privaten Unternehmen ermöglicht, unsere Telefone und unser Leben zu infiltrieren und unbegrenzten Zugang zu persönlichen Informationen zu erhalten. Auch die deutsche Organisation *BDS-Berlin* beteiligt sich an dem weltweiten Aktionstag. Von **Shir Hever**.

Obwohl es sich bei allen Unternehmen, die Spyware aus Profitgründen verkaufen (und nicht an staatliche Geheimdienste liefern), um israelische Firmen handelt, ist Deutschland tief in den Spyware-Skandal verwickelt. Das Bundeskriminalamt (BKA) hat zugegeben, dass es das Pegasus-Programm von der NSO-Gruppe gekauft hat. Das BKA war besorgt darüber, dass mit Pegasus der Polizei ein Zugriff auf mehr Informationen ermöglicht wird, als ein Gerichtsbeschluss zulassen würde, und bat die NSO Group, ein weniger invasives Programm zu liefern. Die NSO Group weigerte sich zunächst, erklärte sich aber schließlich bereit, eine Sperre in ihrem eigenen Programm zu installieren. Nun müssen die Deutschen darauf vertrauen, dass die Polizei diese Sperre nicht umgeht und ihre Macht nicht missbraucht.

Nach Angaben der *Carnegie Endowment* ist Deutschland nach Israel der zweitgrößte Exporteur von Spähsoftware in der Welt (wenn auch mit großem Abstand), was jedoch hauptsächlich auf das deutsche Unternehmen *Finfisher* aus München zurückzuführen ist, das Berichten zufolge seine Tätigkeit eingestellt hat.

Nachdem die Rolle israelischer Spyware, insbesondere der Firma *NSO Group* und ihres schädlichen Programms Pegasus, bei der Ermordung von Jamal Khashoggi 2018, bei der Unterdrückung der Ermittlungen zu den 43 verschwundenen Studierenden in Mexiko – die höchstwahrscheinlich ermordet wurden – und bei weiteren Skandalen in insgesamt 45 Ländern durch die *Washington Post* aufgedeckt wurde, hat das US-Handelsministerium zwei israelische Spyware-Unternehmen auf die schwarze Liste der Unternehmen gesetzt, die die nationalen Interessen der Vereinigten Staaten bedrohen: *NSO Group* und *Candiru*. Dies geschah im November 2021.

Edward Snowden sagte dem *Guardian* bereits im Juli 2021, dass Spionageprogramme gänzlich verboten werden müssen. Aus technischer Sicht kann das Wissen, das zum Hacken eines Telefons eines bestimmten Modells erforderlich ist, leicht dazu verwendet werden, eine beliebige Anzahl von Telefonen desselben Modells zu hacken, wenn die Telefonnummern bekannt sind. Snowden warnte mit dem Hinweis darauf, dass Amnesty International bereits von 50.000 Telefonnummern berichtet hatte, die an die NSO Group gegeben wurden, um sie zu hacken, und außerdem nicht verhindert werden könne, dass es

sehr bald 50 Millionen Telefonnummern sein würden, wenn die Technologie nicht verboten werde.

Snowden warnte, dass die Technologie nicht zur Strafverfolgung eingesetzt werden kann; sie sei so konzipiert, dass sie den Regierungen zu viel Macht gibt und keine Mechanismen der Rechenschaftspflicht enthält. Sie hat eine abschreckende Wirkung auf den Journalismus und hindert Anwälte daran, ihre Gespräche mit Mandanten vertraulich zu behandeln.

Die Möglichkeiten der Kunden von Spionageprogrammen, die Technologie zu nutzen, um Zivilistinnen und Zivilisten (sogar, wenn sie in Journalismus oder als Anwältinnen und Anwälte arbeiten) anzugreifen, sind nahezu unbegrenzt. Das israelische Unternehmen *Intellexa* mit Sitz in Zypern hat Spionageoperationen in Griechenland, Bangladesch und im Sudan durchgeführt. Einer der berüchtigten Kunden von Intellexa ist Mohamed Hamdan Daglo, der zurzeit an einem Putschversuch im Sudan beteiligt ist.

Im Gegensatz zur „normalen“ Spionage, die von staatlichen Stellen wie der CIA, dem FSB und dem BND durchgeführt wird, welche sich in Telefone und E-Mail-Konten einhacken, sind die israelischen Geheimdienste die einzigen, die mit Genehmigung des israelischen Verteidigungsministeriums die aufdringliche Überwachungstechnologie über diese Spyware-Firmen zum Verkauf anbieten. Zu den Kunden israelischer Spyware gehören autoritäre Regierungen in Saudi-Arabien, den Vereinigten Arabischen Emiraten, Belarus, Russland, China (in Hongkong), Äthiopien, Uganda, Honduras und anderen Ländern. Zu den Kunden israelischer Spionagesoftware gehören auch Regierungen, die als demokratisch gelten, wie Griechenland, Deutschland, das Vereinigte Königreich und Spanien.

Die Institutionen der Europäischen Union waren sehr schwach. Das Europäische Parlament setzte im März 2022 den PEGA-Ausschuss ein, um den Einsatz von Spionagesoftware zu untersuchen. Obwohl der Ausschuss feststellte, dass nur israelische Unternehmen Spionageprogramme in der EU verkauft und eingesetzt haben, verfügte er über keinen einzigen hebräischsprachigen Ermittler. Der PEGA-Ausschuss hat ohnehin nicht das Mandat, die Verwendung von Spyware außerhalb der EU zu untersuchen, und er kann nur Empfehlungen aussprechen, die die Europäische Kommission möglicherweise nicht einmal annimmt.

Der einzige EU-Mitgliedsstaat, der entschiedene Maßnahmen ergriffen hat, ist Griechenland. Das Land hat nach dem Skandal, bei dem griechische Politiker mit dem israelischen Spionageprogramm Predator gehackt wurden, Spyware offiziell verboten. Dieses Gesetz ist sehr zu begrüßen, aber es schützt die griechischen Bürgerinnen und Bürger immer noch nicht vor Spionageprogrammen, da die Technologie keine Grenzen

kennt. Zypern ist derzeit der Zufluchtsort für Spyware-Unternehmen, und es gibt nichts, was jemanden in Zypern daran hindern könnte, ein Telefon in Griechenland mit Spyware zu hacken. Die *Carnegie Endowment for International Peace* zitierte einen griechischen Beamten, der sagte: „Wir pissen auf PEGA".

Der PEGA-Ausschuss hat nicht den politischen Willen, ein Verbot von Spyware zu fordern. Aber sein Empfehlungsentwurf fordert ein Verbot des kommerziellen Handels von Telefonen mit Sicherheitslücken, die von den Spyware-Firmen ausgenutzt werden, um die Kontrolle über derlei Geräte aus der Ferne zu übernehmen.

Am 27. März dieses Jahres griff Präsident Biden entschlossener durch und erließ eine Durchführungsverordnung zum Verbot des Verkaufs und der Verwendung kommerzieller Spyware in den USA. Biden beschränkte zwar nicht die Nutzung staatlicher Einrichtungen in den USA zur Entwicklung und Verwendung von Spyware. Aber er argumentierte zu Recht, dass es privaten Unternehmen nicht erlaubt sein sollte, Spyware aus Profitgründen zu verkaufen, da dies die Bürgerrechte der US-Bürger untergräbt. Seine Entscheidung wurde weithin gelobt, auch von *Citizen Lab*, einer in Toronto ansässigen Organisation, die sich auf die Untersuchung der durch Spyware verursachten Schäden und die Durchführung forensischer Untersuchungen kompromittierter Telefone spezialisiert hat.

Am 4. April veröffentlichte die *New York Times* jedoch einen investigativen Artikel, der aufdeckte, dass israelische Spyware-Unternehmen bereits einen Weg gefunden haben, die US-Vorschriften zu umgehen. Nur fünf Tage, nachdem die *NSO Group* im November 2021 auf die Schwarze Liste gesetzt wurde, gründete sie eine Briefkastenfirma mit einem anderen Namen und verkaufte Spionageprogramme an das FBI. Damit wird nicht nur die Schwarze Liste des Handelsministeriums, sondern auch die Durchführungsverordnung vom März lächerlich gemacht.

Spyware ist auch mit der israelischen Desinformationsindustrie verbunden, da israelische Desinformationsunternehmen Spyware als Teil ihres Dienstleistungspakets für die Verbreitung gefälschter Informationen und die illegale Manipulation demokratischer Prozesse einsetzen. Ich habe hier darüber geschrieben. In der Zwischenzeit wurde ein weiterer Desinformationsskandal aufgedeckt, der Deutschland betrifft. Der ehemalige BND-Chef August Hanning war das Ziel einer Desinformationskampagne von Schweizer Konkurrenten, die versuchten, ihn aus dem Amt zu entfernen, indem sie gefälschte Bankdokumente vorlegten, die implizierten, dass Hanning Bankkonten in der Schweiz hatte. Die Schweizer Agenten beschafften die gefälschten Dokumente von der israelischen Desinformationsfirma „Team Jorge", die Tal Hanan gehört. Dies geschah im Jahr 2015, aber die Details werden erst jetzt veröffentlicht. Tal Hanan wurde in der Schweiz verhört, aber es

wurde keine Anklage gegen ihn erhoben. August Hanning sagte, er sei „überrascht“, dass die Israelis ihn ins Visier genommen haben, wenn man bedenkt, wie viel Unterstützung er dem israelischen Mossad über die Jahre gegeben hat. Wenn er wirklich überrascht ist, dann ist es erstaunlich, dass der BND von einer so naiven Person geleitet wurde, die die zynischen Machenschaften des israelischen Geheimdienstes nicht versteht.

Für die Gruppen, die sich an dem weltweiten Aktionstag gegen Spyware beteiligen, bleibt die Frage unbeantwortet, ob Spyware überhaupt von Regierungen bekämpft werden kann. Die Organisationen der Zivilgesellschaft warten nicht darauf, dass die Regierungen zum Schutz der Privatsphäre und der Menschenrechte tätig werden. *Citizen Lab* veröffentlichte am 11. April einen Bericht über das israelische Spyware-Unternehmen *Quadream*, das innerhalb weniger Tage gezwungen war, seine Tätigkeit einzustellen und seine Mitarbeiter zu entlassen. Auch wenn die Regierungen schwach sind, besteht immer noch die Hoffnung, dass der Druck der Bevölkerung dieser schädlichen Technologie ein Ende setzen wird.