Werden die EU und die Pandemie den Weg für eine globale israelische Überwachung ebnen?

Ali Abunimah, electronicintifada.net, 13.04.20

Die Coronavirus-Pandemie ist eine unschätzbare Gelegenheit für Regierungen und Spionage-unternehmen, ihre Einflussmöglichkeiten auf das Leben der Menschen auszuweiten.

Laut Aussage von Gesundheitsbehörden, ist die effektive Rückverfolgung von Kontakten von entscheidender Bedeutung, um die weiträumige Abschottungen zu beenden und neue Ausbrüche des Virus schnell zu stoppen, zumindest bis ein Impfstoff entwickelt ist.

Israels hochgelobte Tech-Industrie ist eng mit dem Militär- und Geheimdienstapparat des Landes verbunden, der PalästinenserInnen unter militärischer Besatzung als unfreiwillige Versuchskaninchen für seine Systeme benutzt, die dann an andere Länder vermarktet werden.

Das bedeutet, dass Überwachungstechnologien, die versprechen, jeden, der dem Virus ausgesetzt ist, schnell zu identifizieren, tatsächlich einen globalen Markt finden könnten und es besteht die Gefahr, dass diese Art der invasiven Überwachung zu einem Dauerzustand wird. Eine Firma, die von dieser Gelegenheit profitieren will, ist Israels berüchtigte NSO-Gruppe, die Firma, die Schadsoftware namens *Pegasus* produziert, die heimlich auf einem Mobiltelefon eines Zielobjekts eingeschleust werden kann.

Diese *Malware* kann dazu benutzt werden, fast alle privaten Informationen an die Spione zurückzuschicken, einschließlich Aufzeichnungen, Bildschirmaufnahmen, Passwörter, E-Mails und Textnachrichten.

Israels hochgelobte Tech-Industrie ist eng mit dem Militär- und Geheimdienstapparat des Landes verbunden, der PalästinenserInnen unter militärischer Besatzung als unfreiwillige Versuchskaninchen für seine Systeme benutzt, die dann an andere Länder vermarktet werden.

Nun sieht es so aus, als ob die europäischen Regierungen bereit sind, die Früchte dieser missbräuchlichen und repressiven Strukturen unter dem Vorwand der Bekämpfung der Pandemie zu übernehmen.

Pegasus, die Schadsware der NSO-Gruppe, die nur an Regierungen verkauft wird, ist in Dutzenden von Ländern gegen Journalisten und Menschenrechtsaktivisten missbraucht worden. Zu den mutmaßlichen Nutzern gehören Marokko, Mexiko, die Vereinigten Arabischen Emirate, Bahrain und Kasachstan.

Bei der Ermordung von Jamal Khashoggi war die Schadsoftware mit involviert. Khashoggi ist der saudische Journalist, der 2018 in das Konsulat seines Landes in Istanbul gelockt und brutal ermordet und zerstückelt wurde.

Amnesty International, dessen Mitarbeiter mit *Malware* der NSO-Gruppe ins Visier genommen wurden, verklagt das Unternehmen, um seine Beteiligung an missbräuchlicher Überwachung zu beenden. Auch *Facebook* verklagt die NSO Group wegen mutmaßlicher Kompromittierung ihrer Messaging-Plattform *WhatsApp*, die Regierungen dabei hilft, rund 1.400 Personen auf vier Kontinenten auszuspionieren.

„Zynischer Versuch“

Nun sind Datenschutz- und Menschenrechtsexperten besorgt darüber, dass die NSO-Gruppe an der Spitze einer von der israelischen Regierung geförderten Initiative zur Überwachung von Coronaviren steht, die in anderen Ländern übernommen werden könnte.

Der israelische Verteidigungsminister Naftali Bennett gab im vergangenen Monat damit an, dass sein Ministerium und das israelische Militär mit der NSO-Gruppe zusammengearbeitet hätten, um ein System zu entwickeln, das den Israelis eine Bewertung der Wahrscheinlichkeit einer Infektion mit dem neuen Coronavirus geben soll.

Laut *Globes*, einer israelischen Fachzeitschrift für Wirtschaft, „wird das System Informationen über Israelis sammeln, in Echtzeit aktualisieren und jedem Israeli eine ‚Infektionseinstufung‘ auf einer Skala von eins bis 10 zuweisen“.

Es gibt besorgniserregende Anzeichen dafür, dass die Europäische Union und ihre Mitgliedstaaten beabsichtigen, israelische Massenüberwachungstechnologie unter dem Deckmantel der Bekämpfung von COVID-19 zu übernehmen.

Die Publikation *Vice* erhielt einen Einblick in die Technologie der NSO-Gruppe. Sie beschreibt das System der *NSO Group* und ein ähnliches, das von der italienischen Firma *Cy4Gate* entwickelt wurde, als „im Wesentlichen Massenüberwachungsinstrumente, die Regierungen und Gesundheitsbehörden dabei helfen würden, die Bewegungen jedes Bürgers zu verfolgen und zu wem diese Kontakt haben“.

Zu diesem Zweck, so *Vice*, hat die *NSO Group* „die Nutzeroberfläche angepasst, ebenso wie das Analysewerkzeug, das sie bereits entwickelt hatten, um es zusammen mit der leistungsstarken *Malware* namens *Pegasus* zu benutzen, um sich in Mobiltelefone einzuhacken und Daten wie Fotos, Mitteilungen und Telefonanrufe aus ihnen herauszulesen.

Das neue System, mit dem Namen *Fleming*, „ermöglicht es Analysten nachzuvollziehen, wohin Menschen gehen, wen sie treffen, für wie lange und wo“. Es werden angeblich willkürliche ID-Nummern an Personen vergeben, um ihre Privatsphäre zu schützen, aber ein Informant der *NSO Group* teilte *Vice* mit, dass die Regierung die Informationen „bei Bedarf“ de-anonymisieren kann. In Wirklichkeit handelt es sich dabei um eine Echtzeitverfolgung jeder Person.

„Dies ist der zynische Versuch einer berüchtigten Spyware-Firma, in die Massenüberwachung einzusteigen“, sagte John Scott-Railton, ein leitender Forscher am *Citizen Lab* der Universität Toronto, gegenüber *Vice*. *Citizen Lab* spielte eine wesentliche forensische Rolle bei der Aufdeckung wie diese *Spyware* der NSO-Gruppe weltweit missbräuchlich eingesetzt wird. „Alle BürgerInnen möchten so schnell wie möglich wieder zum Normalzustand zurückkehren. Der Goldrausch in der Überwachungstechnologie könnte jedoch bedeuten, dass es eine normale Erwartung an eine Privatsphäre gibt, zu der wir nur schwer zurückkehren können“, fügte Scott-Railton hinzu. Laut *Vice*, teilen Mobilfunkbetreiber in Ländern wie Italien, Deutschland, Österreich, Spanien, Frankreich, Belgien und Großbritannien „bereits die Standorte ihrer Kunden mit ihren Regierungen, um die Verbreitung des Virus zu verfolgen“.

Europäischer Enthusiasmus

Es gibt zwar keine Berichte darüber, dass diese Regierungen die Systeme der NSO-Gruppe nutzen, doch gibt es besorgniserregende Anzeichen dafür, dass die Europäische Union und ihre Mitgliedstaaten beabsichtigen, israelische Massenüberwachungstechnologie unter dem Deckmantel der Bekämpfung von COVID-19 zu übernehmen.

Die niederländische Botschaft in Tel Aviv twitterte am Montag, dass sie „auf der Suche nach niederländischen Unternehmen sei, die sich gemeinsam mit einem israelischen Partner um eine einmalige Ausschreibung für intelligente digitale Lösungen für Corona (wie Apps) durch das niederländische Gesundheitsministerium bewerben wollen".

> Looking for [ital. Flagge] companies that want to team up with an [israel. Flagge] partner to apply for a unique tender for smart digital solutions for corona (like [Piktogramm] apps) by the Dutch Ministry of Health. Deadline is 14 April so contact our Innovation Attaché @RacheliInnovate now: racheli@nost.org.il
>
> — Dutch Embassy Israel (@NLinIsrael) April 13, 2020

Emanuele Giaufret, der Botschafter der Europäischen Union in Tel Aviv, veröffentlichte in der Jerusalem Post einen Leitartikel, in dem er darüber schrieb, wie die 27 EU-Mitgliedsstaaten „ihre wissenschaftliche und technologische Forschung nutzt, um COVID-19 zu bekämpfen", und dies die „Kooperationsprojekte mit Israel" einschließe.

> The [EU Flagge] European Union is spearheading the int'l response to the #coronavirus pandemic Read the Op-ed by #EU [EU Flagge] Ambassador @EGiaufretEU ?å https://t.co/sqVRAYiNR4
>
> — EU in Israel [EU und israelische Flagge] (@EUinIsrael) April 13, 2020

Laut Giaufret hat die EU etwa 150 Millionen Dollar aus ihrem Wissenschaftsprogramm *Horizont 2020* bereitgestellt, „um wissenschaftliche Teams in ganz Europa sowie in Partnerländern, darunter Israel, zu finanzieren, die dabei helfen sollen, schnell einen Impfstoff gegen COVID-19 zu entwickeln".

Er fügt hinzu, dass das Ziel der Bemühungen „die Verbesserung von Diagnostik, Vorsorge, klinischem Management und Behandlung ist".

Die wendige Firma *Elbit* präsentiert sich zur Zeit selbst als Anbieter von Technologie zur Bekämpfung der Pandemie. Diese Aktivitäten umfassen auch die Finanzierung von Überwachungsmaßnahmen, insbesondere da *Horizon 2020* in den letzten Jahren bereits genutzt wurde, Gelder an *Elbit Systems*, neben anderen Unternehmen der israelischen Kriegsindustrie, zu leiten. Der israelische Verteidigungsminister Bennett machte deutlich, dass er das Coronavirus Überwachungs-system der NSO-Gruppe exportieren will. *Sky News* berichtete Anfang des Monats, dass die NSO-Gruppe „sich an eine Reihe westlicher Länder gewandt hat, um ihnen ihre Software zur Verfolgung von Coronaviren anzubieten".

An PalestinenserInnen getestet

Israels Misshandlung von PalästinenserInnen, darunter auch seiner eigenen Bürger, während der Corona-Pandemie folgt dem gleichen rassistischen, gewalttätigen und rücksichtslosen Muster, wie es für diesen Staat grundlegend ist.

Israelische Medien haben bestätigt, dass die Einheit für Cyberwarfare *Unit 8200* der israelischen Armee am Coronavirus-Tracking-Projekt der NSO-Gruppe beteiligt ist.

Palästinensische Arbeiter aus dem besetzten Westjordanland haben kaum eine andere Wahl, als für israelische Arbeitgeber zu arbeiten, um ihre Familien zu ernähren. Während sie dort sind, sind sie dem Virus ausgesetzt und riskieren dabei, dass sie ihn in ihre eigenen Gemeinwesen bringen.

Doch die systematische Missachtung der Gesundheit und Sicherheit der Palästinenser durch Israel, hat nicht dazu geführt, sie zu Versuchsobjekten für seine Kontroll- und Überwachungstechnologien zu machen.

Die Zeitung *Haaretz* berichtete letzte Woche darüber, dass „Palästinenser, die überprüfen möchten, ob ihre Aufenthaltsgenehmigungen in Israel noch gültig sind, von Israel dazu aufgefordert wurden, eine App herunterzuladen, die es dem Militär ermöglicht, auf ihre Mobiltelefone zuzugreifen".

„Die App ermöglicht es dem Militär, den Standort des Mobiltelefons der PalästinenserInnen zu verfolgen und auf Benachrichtigungen und Dateien, die sie erhalten, herunterladen und speichern zuzugreifen, sowie auf die Kamera des Geräts."

Haaretz klärt nicht darüber auf, in welcher Weise ein solch invasiver Zugriff etwas mit der Bekämpfung des Virus zu tun hat, und auch nicht darüber, wer diese spezielle App entwickelt hat.

Israelische Medien haben jedoch bestätigt, dass die Einheit für Cyberwarfare *Unit 8200* der israelischen Armee am Coronavirus-Tracking-Projekt der NSO-Gruppe beteiligt ist.

2014 enthüllten Veteranen der *Unit 8200*, dass „die palästinensische Bevölkerung der Spionage und Überwachung durch den israelischen Geheimdienst, unter der Militärregierung vollständig ausgeliefert ist". Sie gaben zu, dass die von ihnen gesammelten und gespeicherten Informationen „unschuldigen Menschen schaden". „Sie dient der politischen Verfolgung und zur Herbeiführung von Spaltungen innerhalb der palästinensischen Gesellschaft, indem sie Kollaborateure rekrutiert und Teile der palästinensischen Gesellschaft gegen sich aufhetzt", fügten die Agenten hinzu. Jetzt kann auch der Rest der Welt die palästinensische Behandlung erfahren.

„Was in Palästina passiert, bleibt nicht in Palästina", merkt *Who Profits* auf einer neuen Webseite an, die der Überwachung der COVID-19-Krise im Kontext der israelischen Besatzung gewidmet ist. „Ein zentraler Grund dafür, dass Israel ständig darum bemüht ist, sein Unterdrückungs-Portfolio zu erweitern, ist, dass es später auch außerhalb angewandt werden kann, um Gewinn und politische Vorteile zu erzielen."

Die Coronavirus-Pandemie bietet Israel die perfekte Gelegenheit, seine Spionage auf genau diese Weise zu vermarkten.

Und alles deutet darauf hin, dass die Europäische Union, im Einklang mit ihrer kontinuierlichen Komplizenschaft, dazu bereit ist, Israel dabei zu helfen, seine Überwachung auf praktisch jeden weltweit auszuweiten.

Quelle:

https://electronicintifada.net/blogs/ali-abunimah/will-eu-and-pandemic-pave-way-israeli-global-surveillance

Siehe auch den Artikel:

Israelischer Spyware-Hersteller will Corona-Tracker verkaufen

https://netzpolitik.org/2020/israelischer-spyware-hersteller-will-corona-tracker-verkaufen/