Wie die israelische Spionagetechnik tief in unser Leben hineinreicht

Israelische Software, die auf Palästinenser angewandt wird, führt zu neuen Cyberwaffen, die in globale digitale Plattformen integriert werden.

Jonathan Cook, Middle East Eye, 11.11.19

Die von Israel entwickelten Waffen des digitalen Zeitalters, die auch zur Unterdrückung der Palästinenser entwickelt wurden, werden rasch für viel breitere Anwendungen, gegen westliche Bevölkerungsgruppen, die ihre Freiheiten längst für selbstverständlich halten, verwendet.

Israels Status als „Startup-Nation“ für Hightech-Innovation, wurde vor Jahrzehnten begründet. Doch sein Ruf hing immer von einer dunklen Seite ab, die immer schwieriger zu ignorieren ist.

Israel ist seit langem weltweit führend in einem extrem lukrativen Waffenhandel und verkauft seine Waffensysteme an autoritäre Regime auf der ganzen Welt als an Palästinensern „kampferprobte“ Waffensysteme

Vor einigen Jahren warnte der israelische Analyst Jeff Halper davor, dass Israel weltweit eine Schlüsselrolle bei der Zusammenführung neuer digitaler Technologien mit seiner Sicherheitsindustrie eingenommen habe. Wir wären alle in Gefahr Palästinenser zu werden.

Er stellte fest, dass Israel Millionen von Palästinensern unter seiner nicht rechenschaftspflichtigen, Militärherrschaft tatsächlich als Versuchskaninchen in Freilandlabors behandle. Sie seien die Testumgebung zur Entwicklung nicht nur neuer konventioneller Waffensysteme, sondern auch neuer Werkzeuge zur Massenüberwachung und -kontrolle.

Wie ein kürzlich in *Haaretz* erschienener Bericht feststellte, sind Israels Überwachungsmaßnahmen der Palästinenser „eine der umfangreichsten ihrer Art weltweit“. Dazu gehören die Überwachung der Medien, der sozialen Medien und der Bevölkerung als Ganzes.

Big-Brother-Handel

Doch was in den besetzten Gebieten anfing, würde nicht auf das Westjordanland, Ost-Jerusalem und auf den Gazastreifen begrenzt bleiben. Es besteht einfach die Möglichkeit, mit dem Handel mit diesen neuen hybriden Formen der offensiven digitalen Technologien Geld zu machen und Einfluss zu gewinnen.

So klein Israel auch sein mag, es ist seit langem weltweit führend in einem extrem lukrativen Waffenhandel und verkauft seine Waffensysteme an autoritäre Regime auf der ganzen Welt als an Palästinensern „kampferprobte“ Waffensysteme.

Der Handel mit militärischer Hardware wird zunehmend von einem Markt für aggressive Software überlagert, nämlich dem Handel mit Werkzeugen für Cyber-Kriege. Solch neuzeitliche Waffen werden von den

Staaten stark nachgefragt, die sie nicht nur gegen externe Feinde einsetzen wollen, sondern auch gegen die eigenen Bürger, die abweichende Meinungen vertreten und Beobachtern bezüglich der Einhaltung der Menschenrechte. Israel kann zu Recht behaupten, hier eine Weltmacht zu sein, die die Bevölkerung unter ihrer Herrschaft kontrolliert und unterdrückt. Israel achtet jedoch darauf, die eigenen Fingerabdrücke von einem Großteil dieser neuen Big-Brother-Technologien fernzuhalten, indem es die Weiterentwicklung dieser Cyber-Werkzeuge an Absolventen seiner berüchtigten Sicherheits- und Militärnachrichtendienste auslagert. Gleichwohl bewilligt Israel solche Aktivitäten implizit, indem es diesen Unternehmen Exportlizenzen erteilt, und die höchsten Sicherheitsbeamten des Landes sind oft eng in diese Arbeit eingebunden.

Spannungen mit Silicon Valley

Nach dem Ausscheiden aus der Armee, können Israelis auf jahrelange Erfahrung mit dem Ausspionieren von Palästinensern zurückgreifen und Unternehmen gründen, die ähnliche Software für allgemeinere Anwendungen entwickeln.

Als Zeichen der Spannungen hat *WhatsApp*, eine *Social-Media*-Plattform die *Facebook* gehört, letzte Woche vor einem kalifornischen Gericht die erste Klage dieser Art gegen Israels größtes Überwachungsunternehmen NSO*, eingereicht.

Apps mit ausgefeilter Überwachungstechnologie aus Israel werden in unseren digitalen Leben immer häufiger eingesetzt. Einige davon werden für relativ harmlose Nutzungen verwandt. *Waze*, das die Verkehrsbelastung aufzeichnet, ermöglicht es den FahrerInnen, schneller ans Ziel zu gelangen, während *Gett* Kunden telefonisch mit Taxis in der Nähe verbindet.

Doch einige der geheimeren Technologien, die von israelischen Entwicklern produziert werden, sind viel näher an ihrem ursprünglichen militärischen Format.

Diese offensive Software wird sowohl an Nationen verkauft, die ihre eigenen Bürger oder Rivalen ausspionieren möchten, als auch an Privatunternehmen, die hoffen, sich einen Vorteil gegenüber Wettbewerbern zu verschaffen, oder ihre Kunden besser kommerziell zu manipulieren.

Ist eine solche Spyware in *Social-Media*-Plattformen mit Milliarden von Nutzern integriert, ist sie für staatliche Sicherheitsbehörden von potenziell globaler Reichweite. Das erklärt die manchmal angespannte Beziehung zwischen israelischen Technologieunternehmen und Silicon Valley, das bemüht ist, Kontrolle über diese *Malware* [Schadsoftware] zu erlangen, wie zwei gegensätzliche, aktuelle Beispiele belegen.

„Spy-Kit“ für Mobiltelefone

Als Zeichen der Spannungen hat *WhatsApp*, eine *Social-Media*-Plattform die *Facebook* gehört, letzte Woche vor einem kalifornischen Gericht die erste Klage dieser Art gegen Israels größtes Überwachungsunternehmen NSO*, eingereicht.

WhatsApp beschuldigt NSO der Cyber-Angriffe. Innerhalb von nur zwei Wochen, die Anfang Mai von *WhatsApp* untersucht wurden, soll NSO die Mobiltelefone von mehr als 1.400 Nutzern in 20 Ländern ins Visier genommen haben.

Pegasus, die *Spyware* [Spionagesoftware] der NSO, wurde gegen Menschenrechtsaktivisten, Anwälte, religiöse Führer, JournalistInnen und MitarbeiterInnen von Hilfsorganisationen eingesetzt. Letzte Woche enthüllte *Reuters*, dass hohe Beamte von US-Verbündeten ebenfalls von der NSO anvisiert wurden.

Nachdem *Pegasus* das Telefon des Benutzers ohne dessen Wissen übernommen hat, kopiert es Daten und schaltet zum Abhören das Mikrofon ein. Laut der Zeitschrift *Forbes* ist es „das invasivste mobile Spionage-Set der Welt".

NSO hat die Software an Dutzende von Regierungen lizenziert, darunter solche, die für Menschenrechtsverletzungen bekannt sind, wie Saudi-Arabien, Bahrain, die Vereinigten Arabischen Emirate, Kasachstan, Mexiko und Marokko.

Auch Amnesty International hat sich darüber beschwert, dass seine MitarbeiterInnen von der NSO-Spionagesoftware angegriffen wurden. Zur Zeit unterstützt AI eine Klage gegen die israelische Regierung, weil sie dem Unternehmen eine Ausfuhrgenehmigung erteilt hat.

Verbindungen zu israelischen Sicherheitsdiensten

2010 wurde NSO von Omri Lavie und Shalev Hulio gegründet, beide bekannt als Absolventen von Israels vielgepriesener militärischen Geheimdiensteinheit *8200*.

Im Jahr 2014 enthüllten Whistleblower, dass die Einheit routinemäßig Palästinenser ausspionierte, ihre Telefone und Computer durchstöberte, um Beweise für sexuelles Fehlverhalten, Gesundheitsprobleme oder finanzielle Schwierigkeiten zu finden, die dazu dienen könnten, sie zur Zusammenarbeit mit den israelischen Militärbehörden zu erpressen.

Die Soldaten schrieben, dass die Palästinenser „der Spionage und Überwachung durch den israelischen Geheimdienst komplett ausgesetzt seien. Die Spionagesoftware wird zur politischen Verfolgung und zu Spaltungen innerhalb der palästinensischen Gesellschaft eingesetzt, indem sie Kollaborateure rekrutiert und Teile der palästinensischen Gesellschaft gegen sich selbst aufhetzt."

Trotz der Erteilung von Ausfuhrgenehmigungen an die NSO durch Regierungsbeamte, bestritt der israelische Minister Zeev Elkin letzte Woche eine „israelische Regierungsbeteiligung" an dem Angriff auf *WhatsApp*. Gegenüber dem israelischen Radio erklärte er: „Jeder weiß, dass dies nichts mit dem Staat Israel zu tun hat."

Von Kameras verfolgt

In der gleichen Woche, in der *WhatsApp* die Klage einreichte, enthüllte der US-Fernsehsender NBC, dass *Silicon Valley* dennoch daran interessiert sei, israelische *Start-Ups* zu kontaktieren, die tief in Missbrauch im Zusammenhang mit der Besatzung verwickelt sind.

Microsoft hat erheblich in *AnyVision* investiert, um die bereits hochentwickelte Gesichtserkennungstechnologie weiterzuentwickeln, die dem israelischen Militär dabei hilft, Palästinenser zu unterdrücken.Die Verbindungen zwischen *AnyVision* und den israelischen Sicherheitsdiensten sind kaum zu übersehen. Tamir Pardo, ehemaliger Leiter der israelischen Spionagebehörde Mossad, gehört zu seinem Beirat. Amir Kain, Präsident des Unternehmens, war zuvor Leiter von *Malmab*, der Sicherheitsabteilung des Verteidigungsministeriums.

AnyVisions Hauptsoftware *Better Tomorrow*, hat den Spitznamen „Besatzungs-Google“, weil die Firma behauptet, dass sie jeden Palästinenser identifizieren und verfolgen kann, indem sie Filmmaterial aus dem umfangreichen Netzwerk von Überwachungskameras in den besetzten Gebieten auswerten kann.

Große Sorge

Trotz der offensichtlichen ethischen Probleme, legen die Investitionen von Microsoft nahe, dass es sich zum Ziel gesetzt hat, die Software in seine eigenen Programme zu integrieren. Bei Menschenrechtsorganisationen hat dies zu großer Besorgnis geführt.

Die israelische Regierung hat ein wachsendes Interesse an der Nutzung dieser Spionage-technologien auch in USA und Europa, da seine Besatzung zum Mittelpunkt von Kontroversen und Untersuchungen im politischen Mainstream-Diskurs geworden ist

Shankar Narayan von der *American Civil Liberties Union* hat vor einer Zukunft gewarnt, die den PalästinenserInnen, die unter israelischer Herrschaft leben allzu bekannt ist: „Der weit verbreitete Einsatz von Gesichtsüberwachung stellt die Prämisse der Freiheit auf den Kopf und die Gesellschaft wird zu einer in der jede/r verfolgt wird, egal was er/sie tut, und das die ganze Zeit“, sagte Narayan gegenüber NBC „Gesichtserkennung ist möglicherweise das perfekteste Werkzeug zur kompletten Regierungskontrolle in öffentlichen Räumen“.

Laut Yael Berda, einem Forscher an der Harvard University, führt Israel eine Liste von rund 200.000 Palästinensern im Westjordanland, die rund um die Uhr überwacht werden sollen. Technologien wie *AnyVision* werden als unverzichtbar dafür angesehen, diese riesige Gruppe unter ständiger Beobachtung zu halten.

Ein früherer Angestellter von *AnyVision* sagte NBC gegenüber, dass die PalästinenserInen behandelt würden, wie eine Testumgebung. „Die Technologie wurde in einer der anspruchsvollsten Sicherheits-umgebungen der Welt im praktischen Einsatz getestet und wir haben sie nun auf den übrigen Markt gebracht“, sagte er.

Wahlmanipulationen

Die israelische Regierung hat ein wachsendes Interesse an der Nutzung dieser Spionagetechnologien auch in USA und Europa, da seine Besatzung zum Mittelpunkt von Kontroversen und Untersuchungen im politischen Mainstream-Diskurs geworden ist.

In Großbritannien wurde der Wandel des politischen Klimas durch die Wahl von Jeremy Corbyn, zum Vorsitzenden der oppositionellen Labour Party deutlich, der ein langjähriger Vertreter palästinensischer Rechte ist. In den USA ist vor kurzem eine kleine Gruppe von Abgeordneten, die die palästinensische Sache offensichtlich unterstützen, in den Kongress gekommen, darunter Rashida Tlaib, die erste palästinensisch-amerikanische Frau, in diesem Amt.

Generell befürchtet Israel die schwunghafte internationale Solidaritätsbewegung BDS (Boykott, Desinvestitionen und Sanktionen), die einen Boykott Israels nach dem Vorbild des Boykotts gegen Apartheid-Südafrika fordert, bis es aufhört, die Palästinenser zu unterdrücken. Die BDS-Bewegung ist stark in vielen Universitäten in den USA gewachsen. Infolgedessen wurden israelische Cyberfirmen immer mehr in die Bestrebungen einbezogen, den öffentlichen Diskurs über Israel zu manipulieren, offenbar auch durch Einmischung in ausländische Wahlen.

Privater „Mossad zum anheuern“

Zwei berüchtigte Beispiele für solche Unternehmen haben kurz für Schlagzeilen gesorgt. Die *Psy-Group*, die sich als „privater Mossad zum Anheuern“ vermarktet hatte, wurde im vergangenen Jahr abgemeldet, nachdem das FBI begonnen hatte, es wegen Einmischung in die US-Präsidentschaftswahl 2016 zu untersuchen. Sein *Project Butterfly*, so der New Yorker, zielte darauf ab, „antiisraelische Bewegungen von innen zu destabilisieren und durcheinander zu bringen“.

Im vergangenen Jahr wurde *Black Cube* entlarvt, weil es eine feindliche Überwachung führender Mitglieder der früheren US-Regierung während der Regierung von Barack Obama durchgeführt hatte. Es scheint eng mit den israelischen Sicherheitsdiensten verbunden zu sein und befand sich eine Zeit lang auf einer israelischen Militärbasis.

Von *Apple* verboten

Es gibt noch andere israelische Unternehmen, die versuchen die Grenze zwischen privatem und öffentlichem Raum zu verwischen. Im Jahr 2913 wurde *Onavo*, ein israelisches Datenerhebungsunternehmen, das von zwei Veteranen der *Unit 8200* gegründet wurde, von *Facebook* übernommen. *Apple* verbot seine VPN-App im letzten Jahr, weil bekannt wurde, dass sie unbegrenzten Zugriff auf die Daten der Benutzer bereitstellt.

Laut einem Bericht in *Haaretz* hatte Gilad Erdan, Israels Minister für strategische Angelegenheiten, der eine geheime Kampagne zur Dämonisierung ausländischer BDS-Aktivisten leitet, im vergangenen Jahr regelmäßige Treffen mit einer anderen Firma namens *Concert*. Diese verdeckt operierende Firma, die von den Gesetzen zur Informationsfreiheit Israels ausgenommen ist, erhielt von der israelischen Regierung finanzielle Mittel in Höhe von rund 36 Millionen Dollar. Seine Direktoren und Aktionäre sind ein *who's who* der israelischen Sicherheits- und Nachrichtenelite. Eine weitere führende israelische Firma, *Candiru*, die nach einem kleinen Amazonas-Fisch benannt ist, der angeblich heimlich in den menschlichen Körper eindringt, wo er zu einem Parasiten wird. *Candiru* verkauft seine Hacker-Werkzeuge hauptsächlich an westliche Regierungen, auch wenn seine Aktivitäten von Ver-schwiegenheit geprägt sind.

Die Mitarbeiter der Firma stammen fast ausschließlich von *Unit 8200*. Ein Hinweis dafür, wie eng die öffentlichen und verdeckten Technologien israelischer Unternehmen sind, gilt die Tatsache, dass *Candiru*-Chef Eitan Achlow, der zuvor die Taxidienst-App *Gett* leitete, die Technologie entwickelt hat.

Dystopische Zukunft

Die israelische Sicherheitselite profitiert von diesem neuen Markt für Cyber-Kriegsführung und nutzt - wie beim Handel mit konventionellen Waffen - eine vorhandene und gefangene palästinensische Bevölkerung, an der sie ihre Technologie testen kann.

Es ist nicht verwunderlich, dass Israel in den westlichen Ländern allmählich invasive und repressive Technologien normalisiert, die den Palästinensern seit langem vertraut sind.

Die Software zur Gesichtserkennung ermöglicht eine immer anspruchsvollere Erstellung von Rassenprofilen, sowie eine politische Profilerstellung. Verdeckte Datenerfassung und -überwachung zerstört die traditionellen Grenzen zwischen privatem und öffentlichem Raum. Die daraus resultierenden *Doxxing*-Kampagnen machen es leicht, diejenigen einzuschüchtern, zu bedrohen und zu schwächen, die andere Meinungen vertreten, und wie die Verteidiger der Menschenrechte, versuchen, die Mächtigen zur Verantwortung zu ziehen. [*Doxxing* ist die internetbasierte Praxis der Recherche, Zusammenstellung und Übertragung privater oder identifizierender Informationen, insbesondere personenbezogener Daten.]

Wenn sich diese dystopische Zukunft weiter ausbreitet, werden New York, London, Berlin und Paris mehr und mehr wie Nablus, Hebron, Ost-Jerusalem und Gaza aussehen. Und wir werden alle verstehen, was es bedeutet, in einem Überwachungsstaat zu leben, der sich im Cyber-Krieg gegen diejenigen befindet, über die er herrscht.

Übersetzung: M. Kunkel, Pako – palaestinakomitee-stuttgart.de

Quelle: https://www.jonathan-cook.net/2019-11-11/israel-spy-tech-cyber/

Für weitere Informationen siehe auch die Artikel:

***Israel's NSO: The shadowy firm behind the 'chilling' spyware used to hack WhatsApp and cloud services**

https://www.telegraph.co.uk/technology/2019/05/14/israels-nso-shadowy-firm-behind-chilling-spyware-used-hack-whatsapp/

und

Facebook Sues Israeli Cyber Security Co. NSO Over WhatsApp Surveillance

Interview mit Dr. Shir Hever
https://therealnews.com/stories/facebook-sues-israeli-cyber-security-co-nso-over-whatsapp-surveillance