

Israelische Unternehmen verkaufen Spionagetechnologie, die sie für die Besetzung Palästinas entwickelt haben

Interview von *The Real News* mit Antony Loewenstein, 20. 01.19, Transkript

GREG WILPERT: Hier ist The Real News Network, ich bin Greg Wilpert, der aus Baltimore zu Ihnen spricht.

Wir sprechen mit Antony Loewenstein, Autor eines Artikels über "Exporting the Technology of Occupation". Er zeigt die wachsende Verbindung zwischen israelischen offensiven Cyberunternehmen und der Massenüberwachung im Dienste autoritärer Regierungen auf der ganzen Welt.

In den letzten 10 Jahren gab es drei große Kriege in Gaza. Und gerade die Unternehmen, die diese Geräte und Technologien verkaufen, sagen, dass sie im Kampf getestet wurden

Eine kleine Anzahl israelischer Unternehmen spielt eine wachsende Rolle bei der Verfolgung von Menschenrechtsaktivisten in Mexiko, bei der Ermordung des Journalisten der Washington Post, Jamal Khashoggi, in Istanbul, beim Versuch von Harvey Weinstein, Frauen zum Schweigen zu bringen, die sich über seine sexuelle Belästigung beschwert haben, und generell bei der Unterstützung autoritärer Regierungen auf der ganzen Welt, damit sie ihre Macht behalten. Nun sprach der israelische Premierminister Benjamin Netanyahu im vergangenen Jahr über die Rolle Israels auf dem globalen Cybersicherheitsmarkt.

Ausschnitt aus einer Netanyahu-Rede:

BENJAMIN NETANYAHU: Israel erhält heute etwa 20 Prozent der globalen Investitionen, privaten Investitionen, in die Cybersicherheit. Das ist viel, wenn man bedenkt, dass wir ein Zehntel von 1 Prozent der Weltbevölkerung sind. Das bedeutet, dass wir etwa 200-mal über unserem Gewicht punkten. Hier sind die Verkäufe, die wir tatsächlich erhalten haben. Du siehst, wie es nach oben geht. Es wird immer weiter nach oben gehen, wegen der steigenden privaten Investitionen in Israel aufgrund der offensichtlichen Notwendigkeit und der Tatsache, dass Israel zu einem Brennpunkt geworden ist. Mein Ziel war es, Israel vor acht Jahren zu einer der fünf führenden Cybermächte der Welt zu machen. Ich glaube, das haben wir erreicht. Ich denke, wir sind auf dieser Liste vielleicht sogar noch weiter vorne.

GREG WILPERT: Ein neuer Artikel in *The New York Review of Books* zeigt, wie der wachsende Cybersicherheitssektor in Israel wächst und wie diese Technologie in Länder und an fragwürdige Personen auf der ganzen Welt verkauft wird. Er wurde von Antony Loewenstein geschrieben und trägt

den Titel „Export der Technologie der Besetzung“. Was ist also der Grund dafür, dass so viel von der Cybersicherheitstechnologie aus Israel kommt, und wie wirkt sie sich auf unser Leben aus? Bei der Diskussion dieser Fragen werden wir von Antony Loewenstein, dem Autor des Artikels, unterstützt. Antony ist ein unabhängiger Journalist und Autor des Buches „Disaster Capitalism: Making a Killing Out of Catastrophe“. Danke, dass du wieder bei uns bist, Antony.

ANTONY LOEWENSTEIN: Danke.

GREG WILPERT: Apropos Besetzung: Inwiefern stellt die Besetzung palästinensischer Gebiete und Bevölkerungsgruppen einen kommerziellen Vorteil für diese israelischen Cybersicherheitsfirmen dar?

ANTONY LOEWENSTEIN: Innerhalb von 50 Jahren, seit Israel mit der Besetzung des Westjordanlandes und des Gazastreifens begonnen hat, hat Israel in gewisser Weise, so denken sie jedenfalls, die Idee der Erhaltung und Kontrolle einer Bevölkerung perfektioniert, die sie nicht wollen, nämlich die Palästinenser. So haben in den letzten 20 Jahren verschiedene israelische Unternehmen und die israelische Regierung Wege gefunden, durch diverse Methoden - Sensoren, Drohnen, Mauern, Barrieren, eine unerwünschte Bevölkerung zu verwalten.

Israel verfügt über eine unglaublich fortschrittliche Überwachungstechnologie, mit der es die unter Besetzung stehenden Palästinenser überwacht. Und tatsächlich wird ihre Technologie vor allem in den letzten Jahren oft genutzt, um Menschen auf Facebook zu überwachen

Was sie damit gemacht haben, besonders seit Netanyahu wieder Präsident wurde, ist im Wesentlichen, diese Technologie und diese Methoden an die Welt zu verkaufen. Sie tun dies, indem sie sagen, dass etwas „kampferprobt“ ist. So werden beispielsweise Waffen und Drohnen in Gaza getestet. In den letzten 10 Jahren gab es drei große Kriege in Gaza. Und gerade die Unternehmen, die diese Geräte und Technologien verkaufen, sagen, dass sie im Kampf getestet wurden.

Dies gilt insbesondere für den Bereich der Cybersicherheit, der in den letzten fünf Jahren stark ausgebaut wurde. Wir haben viele israelische Einzelpersonen, ausländische Generäle, Sicherheitsanalysten, die früher in einigen der heimlichstesten israelischen Cybersicherheitszonen gearbeitet haben, die diese Informationstechnologie in den privaten Sektor bringen, mit immer noch sehr, sehr engen Verbindungen zum israelischen Staat.

So zum Beispiel die Idee der Kontrolle und Überwachung - die Fähigkeit, beispielsweise das Smartphone eines anderen zu überwachen, sei es ein iPhone oder ein Android-Handy, ohne dass Sie es überhaupt merken. Und es gibt unzählige Beispiele, Sie haben einige davon in der Einleitung erwähnt, in Mexiko, der Tod von Jamal Khashoggi. Ein Kollege von ihm in Kanada, ein saudischer Dissident, anscheinend wurde sein Telefon von Saudis gehackt, mit einer Technologie, die von den Israelis verkauft worden war. Und deshalb wussten die Saudis genau, wohin Khashoggi gehen würde und was

er sagen würde. So hat Israel in gewisser Weise seine jahrzehntelange Erfahrung mit der Besetzung genutzt und diese weltweit an Länder verkauft, die diese Idee für sehr attraktiv halten.

GREG WILPERT: So veröffentlichte die israelische Zeitung *Haaretz* kürzlich Interviews mit Arbeitern von Black Cube, von der NSO Group und auch mit Arbeitern der verschwiegeneren Candiru Company, die ihren Namen oft ändert. Aus diesen Interviews geht hervor, dass israelische Unternehmen sehr bereit sind, Vereinbarungen mit repressiven autoritären Regierungen zu treffen, um Industriespionage zu betreiben, und dass sie ziemlich unbesorgt sind über den Schaden, den dies ihrem Ruf zufügen könnte. Zeigen israelische Unternehmen weniger Interesse an ethischen Verstößen als nicht-israelische Unternehmen? Und wenn ja, warum ist das so?

ANTONY LOEWENSTEIN: Wenn Sie sich die Top 10 ansehen, zum Beispiel Militärdienstleister in der Welt, ist Israel nur ein einziger. Offensichtlich ist Russland präsent, es gibt die USA, die bei weitem die wichtigsten sind, man hat Frankreich, viele andere Länder. Alle von ihnen verkaufen Waffen an repressive Regime. Daran besteht kein Zweifel. Auf dieser Ebene ist Israel also nicht einzigartig.

Die Cybersicherheits-, Nachrichten- und Überwachungstechnologie wird jedoch vor allem von Israel und den USA vorangetrieben. Die Erfahrung Israels in diesem Bereich ist, wie ich bereits sagte, zum Teil auf Jahre der Besetzung zurückzuführen und das Erlernen dieser Technologien zur Überwachung der Palästinenser im Westjordanland und im Gazastreifen, aber auch in Israel selbst. Israel verfügt über eine unglaublich fortschrittliche Überwachungstechnologie, mit der es die unter Besetzung stehenden Palästinenser überwacht. Und tatsächlich wird ihre Technologie vor allem in den letzten Jahren oft genutzt, um Menschen auf Facebook zu überwachen. Und oft werden Menschen sogar nur deshalb verhaftet, weil sie einen Beitrag auf Facebook geschrieben haben.

Ist Israel also auf diesem Gebiet einzigartig? Ja und nein. Wichtig ist auch zu sagen, dass eines der Themen, die Israel immer mehr entdeckt, darin besteht, dass es andere Länder wie Russland gibt, das jahrelange Erfahrung im Kampf mit dem Assad-Regime in Syrien hat, das jetzt auch seine Waren - in der Regel privat, aber auch öffentlich - als kampferprobt bewirbt. Israel ist also besorgt, denke ich, dass sie, wenn sie nicht ständig die Grenzen überschreiten, um das so zu sagen, und an immer mehr Regime verkaufen, hinterherhinken werden und zurückfallen werden.

Und auch nicht unwichtig ist, dass Israel dies für diplomatische Zwecke nutzt; einer der Gründe, warum Netanyahu Waffen verkauft und diese Überwachungstechnologie an viele repressive Regime weiterreicht, ist es zu versuchen, diplomatische Unterstützung zu erhalten. So treibt er beispielsweise in den letzten Jahren den enorm wichtigen Markt in Afrika voran; mit repressiven Regimen, die ihre eigenen Bürger töten und überwachen. Israel will mehr Unterstützung innerhalb der Vereinten Nationen erhalten. Wann immer es eine UN-Abstimmung über Israel gibt, ist normalerweise die ganze Welt auf der einen Seite und die andere Seite bilden die USA, Israel, Mikronesien, vielleicht Australien. Sie wollen mehr Länder auf der anderen Seite haben. Diese Art von Technologie wird auch aus geopolitischen Gründen eingesetzt.

GREG WILPERT: Nun, die kanadische Organisation *Citizen Larned* hat Beweise dafür gefunden, dass diese Gruppe und andere Unternehmen, die die Telefone hacken, Bürger verschiedener Länder sind. Die Programme, die für solche Angriffe wie Pegasus entwickelt wurden, könnten so tödlich sein wie

jede Bombe oder Rakete, wie wir es im Falle des Mordes an Jamal Khashoggi gesehen haben. Welche Art von Schutz gibt es, um diese Technologie zu kontrollieren und zu regulieren und die Privatsphäre und die Bürgerrechte von Privatpersonen aus den Ländern der Welt zu schützen?

ANTONY LOEWENSTEIN: Nun, es gibt ein paar Antworten darauf. Journalisten, mit denen ich spreche, machen oft Witze, dass der sicherste Weg, heutzutage zu kommunizieren, der mit Stift und Papier sei. Natürlich ist das für viele, viele Menschen, die mit Menschen auf der ganzen Welt kommunizieren wollen, nicht sehr praktisch. Aber es gibt ein Element der Wahrheit darin, dass die Kommunikation heutzutage über jede Art von Gerät - ein Telefon, ein Computer -tatsächlich niemals zu 100 Prozent sicher sein kann. Allerdings gibt es bestimmte Apps. Signal, im Moment ist es eine Kommunikations-App am Telefon, ist anscheinend sicher, soweit wir wissen. Whatsapp ist es aber anscheinend nicht. **Und das wissen wir auch, weil zum Beispiel die Saudis, wie gesagt, mit israelischer Technologie das Telefon eines Dissidenten, eines Kollegen von Jamal Khashoggi, gehackt haben.**

Eine der Dinge, die Leute auch tun können, ist denke ich, natürlich die Verschlüsselung ihrer Nachrichten. Und ich denke auch, dass die Kommunikation auf bestimmten Plattformen - wie zum Beispiel dem Facebook Messenger - sehr unsicher ist. Wenn du also auf diese Weise kommunizierst, spielt es keine Rolle, wenn es nur eine Art Scherz mit Familie oder Freunden ist, es sei denn, du hast sehr private Gedanken, die du für dich behalten willst. Aber seien Sie sich bewusst, dass es sehr wenig gibt, was man tun kann. Und in der Tat, hat Edward Snowden, der ehemalige NSA Whistleblower, Jahre damit verbracht, Wege zu finden, um ein fast hackfreies Telefon zu entwickeln. Es gibt diese Telefone. Sie sind immer auf einem separaten Betriebssystem, fernab von Apple und Android. **Und ich denke, dass im Laufe der Jahre immer mehr Menschen sich der Komplizenschaft vieler dieser Kommunikationsunternehmen bei der Überwachung bewusst werden - Facebook, Google, Apple - wie kommen wir eigentlich von solchen Unternehmen weg und finden tatsächlich eine Alternative, wo wir sicher kommunizieren können?**

Journalisten und Aktivisten, oder einfach nur Menschen, jeder, der irgendwo kommunizieren will, sollte sich also sehr bewusst sein, dass es fast unmöglich ist, 100 Prozent sicher zu kommunizieren, mit der aktuellen Technologie, die die meisten von uns verwenden, was eine sehr traurige Realität ist.

GREG WILPERT: Nun, wir werden es vorerst dabei belassen. Ich habe mit dem unabhängigen Journalisten Antony Loewenstein gesprochen, dem Autor des Artikels „Exporting the Technology of Occupation“. Nochmals vielen Dank, dass du heute bei uns warst.

ANTONY LOEWENSTEIN: Danke, dass ich kommen durfte.

GREG WILPERT: Und danke, dass Sie sich dem Real News Network angeschlossen haben.

Übersetzung: Pako – palaestinakomitee-stuttgart.de

Quelle:

therealnews.com/stories/israeli-companies-sell-spy-tech-they-perfected-for-occupying-palestine