Pegasus - die Spitze des Eisbergs

03.09.2021

Categories: Apartheid und Siedlungskolonialismus, Militärembargo, Überwachungstechnologie

Seit Jahren untersucht das Citizen's Lab der Universität Toronto das israelische Unternehmen NSO, das sich auf Cyberspionage spezialisiert hat. Im Jahr 2018, nach der brutalen Ermordung des Oppositionellen Jamal Khashoggi in der saudischen Botschaft in Istanbul, tauchte der Name von NSO in den Nachrichten auf. In den letzten Wochen war NSO mit seinem Vorzeigeprodukt Pegasus, einer israelischen Cyberspionage-Software, in vielen Medien in den Schlagzeilen.

Das "Pegasus-Projekt" ist eine Untersuchung von Journalist*innen und Medien in 10 Ländern, die von Forbidden Stories (1) koordiniert wird, einer Medienorganisation in Paris, "deren Aufgabe es ist, die Arbeit anderer Journalist*innen, die bedroht, inhaftiert oder ermordet wurden, zu schützen, weiterzuführen und zu veröffentlichen". Die technische Unterstützung von Amnesty International half, Spuren der Software auf 50.000 Telefonnummern potenzieller Zielpersonen zu identifizieren. Es wurde festgestellt, dass die Spionagesoftware der NSO-Gruppe dazu verwendet wurde, Menschenrechtsverletzungen in großem Umfang auf der ganzen Welt zu erleichtern. Staatsoberhäupter, Journalist*innen, Oppositionelle und Menschenrechtsverteidiger*innen wurden oder werden ins Visier genommen. Kürzlich deckte RTS auf, dass die Schweizer Regierung "Regierungssoftware" (GovWare) verwendet, um Telefone auszuspionieren. Nach Angaben der NZZ handelt es sich dabei um Pegasus.

Alle Medien haben berichtet, dass es sich bei NSO um ein israelisches Unternehmen handelt, aber ohne zu erwähnen, welches die Grundlage für Israels rasante Entwicklung nicht nur der traditionellen Waffenindustrie, sondern auch von Überwachungs- und Spionagewaffen ist.

Viele der innovativsten Technologien, die von der israelischen Zivilindustrie entwickelt wurden, insbesondere im Bereich der Telekommunikation, sind aus der Militärtechnologie abgeleitet. Dieser grundlegende Aspekt wird in den Medienberichten verschwiegen. Ja, Pegasus ist Software, aber vor allem ist es eine neue Waffe aus der israelischen Militärtechnologie. Die Rüstungs- und Sicherheitsindustrie entwickelt und liefert Waffen, die für die Politik der Besatzung, Kolonisierung und Apartheid in Israel/Palästina benötigt werden. Diese Waffen liefern die technischen Mittel für die Unterdrückung der palästinensischen Bevölkerung.

Die israelischen High-Tech-Sektoren verzeichnen die höchsten Wachstumsraten, die in den letzten Jahren durchschnittlich 8 % pro Jahr betrugen. Wie im Waffensektor sind 80 % der Hightech-Produktion für den Export bestimmt. Diese Sektoren erfordern jedoch ein hohes Maß an Qualifikationen und einen hohen Kapitaleinsatz. Auch Forschung und Entwicklung spielen eine wichtige Rolle. Es ist daher nicht verwunderlich, dass Israel 4,9 % seines BIP für diesen Sektor aufwendet, den höchsten Prozentsatz unter den OECD-Ländern. Nach Angaben von UN-Experten gehört Israels Forschungs- und Entwicklungssektor zu den 10 besten der Welt. Ein Großteil der Grundlagenforschung und Entwicklung wird von universitären

Forschungsinstituten geleistet.

Zusammenarbeit zwischen Universitäten und dem israelischen Militär

Die israelischen Sicherheitskräfte, sowohl die öffentlichen als auch die privaten, sind in zunehmendem Maße von Hightech-Geräten aus israelischen Universitäten abhängig. Neue Technologien helfen Israel, seine Besatzung mit weniger Militärpersonal durchzusetzen, und liefern gleichzeitig neue Exportprodukte (Waffen) für die israelische Industrie. Zu den Universitäten, die mit der Rüstungsindustrie zusammenarbeiten, gehören das Technion in Haifa, das Weizman-Institut in Rehovot, die Ben-Gurion-Universität, die Universität Tel Aviv und die Hebräische Universität Jerusalem (HUJ) (3). Letztere bietet auf ihrem illegal in Ostjerusalem gelegenen Campus ein dreijähriges Ausbildungsprogramm (Havatalot) für angehende Offiziere für den Nachrichtendienst im Rahmen ihrer Wehrpflicht an. Diese Soldaten leben auf dem Campus in einem besonderen Bereich und tragen während des Unterrichts ihre Militärkleidung(4). Es gibt nur wenige Länder auf der Welt, in denen das militärische Establishment so eng mit der akademischen Welt und der Wirtschaft zusammenarbeitet, was allen drei Bereichen zugute kommt. Dies hindert die HUJ nicht daran, sich am Programm Horizon 2020 der Europäischen Union zu beteiligen!

Innerhalb der israelischen Verteidigungskräfte (IDF) spielt die Einheit 8200 eine zentrale Rolle bei der Entwicklung neuer Waffen, die für die äußere und innere Verteidigung des Landes als unerlässlich gelten. Die Einheit 8200 rekrutiert die begabtesten jungen Menschen, die für die Entwicklung von Angriffs- und Verteidigungswaffen für Cyber-Spionage und Hacking ausgebildet werden. Später werden sie zahlreich die Armee verlassen, um entweder ihre eigenen Start-ups zu gründen oder um in Unternehmen wie NSO, Quadri, Cyberx usw. einzusteigen. Dank der beruflichen und persönlichen Kontakte, die sie während ihres Militärdienstes geknüpft haben, verfügen die Soldat*innen der Einheit 8200 über gute Voraussetzungen, um die notwendigen Investitionen für die Gründung von Start-ups im Bereich der Cyber-Spionage zu erhalten. Eine von Haaretz zitierte Studie aus dem Jahr 2018 schätzt, dass 80 % der 2.300 Personen, die die 700 israelischen Unternehmen für Cyber-Sicherheit gegründet haben, aus dem Geheimdienst der IDF stammen(7). Und unter den verschiedenen High-Tech-Sektoren wächst die Cybersicherheit rasant. Die Investitionen in den Sicherheitssektor sind im Jahr 2020 um 70 % gestiegen (2,9 Milliarden Dollar).(5)

Cyber-Spionage, eine unverzichtbare Waffe der israelischen Politik

Die Cyberspionage-Industrie ist jedoch nicht nur ein wichtiger Trumpf für die israelische Armee und Wirtschaft, sondern auch ein wichtiges Instrument der Regierungspolitik. Das „Israel National Cyber Directorate“, eine Regierungsbehörde, ist für die Förderung der Kapazitäten des Cyber-Sicherheitssektors des Landes und der inneren Verteidigung zuständig. Bei jedem ausländischen Kaufvertrag übt diese Agentur die Kontrolle während des Ausschreibungsverfahrens, bei der Unterzeichnung des Vertrags und schließlich beim Verkauf aus. Auch der Verkauf von Pegasus, einer Waffe vergleichbar mit Drohnen, Flugzeugen usw., unterliegt diesen Kontrollen. In dem Vertrag, den Pegasus mit seinen Kund*innen abschließt, verpflichten sich diese zwar, bestimmte Regeln einzuhalten, aber es hängt vom guten Willen der Kundschaft ab, sich auch daran zu halten. In Wirklichkeit hat die Regierung kein Interesse daran, den Verkauf zu kontrollieren. Im Gegenzug für die von der Regierungsbehörde genehmigten Ausfuhren erhält Israel politische Vorteile, die sich in der Regierungspolitik niederschlagen.

DarkMatter wurde 2015 in den Vereinigten Arabischen Emiraten (VAE) gegründet und ist offiziell auf Cyberabwehr beschränkt. Laut einer Reuters-Recherche bietet DarkMatter jedoch dem Geheimdienst des Landes Hackerdienste gegen westliche Ziele, Journalist*innen und Menschenrechtsaktivist*innen an. Im Jahr 2020 unterzeichneten Israel und die VAE dank Trumps guter Dienste ein Abkommen zur Aufnahme diplomatischer Beziehungen zwischen den beiden Ländern.

Saudi-Arabien steht auf Israels Liste der feindlichen Länder. Dies hindert Israel jedoch nicht daran, den

Verkauf von schweren Waffen und Cyberwaffen an saudische Unternehmen zuzulassen. Es liegt im Interesse Israels, inoffizielle Kontakte zu bestimmten arabischen Ländern zu unterhalten. Denn feindliche Länder können auch einen gemeinsamen Feind haben, den Iran.

Angesichts der Bedeutung der Ausfuhr von Überwachungs-, Telekommunikations- und Cyberspionage-Waffen (zwischen 7 und 9 % der israelischen Rüstungsexporte) ist die Regierung bestrebt, diese Exporte zu steigern. Iran, Libanon und Syrien sind die einzigen Länder, die davon ausgeschlossen sind.

Und die Schweiz?

Im Jahr 2013 unterzeichnete das EJPD (Eidgenössisches Polizei- und Justizdepartement) einen Vertrag für das neue Schweizer Telefonabhörsystem mit Verint, einem israelischen Unternehmen, das auf Telefonabhörung und Spionage spezialisiert ist. Und das, obwohl die bevorzugte Partnerin von Verint die US-amerikanische National Security Agency (NSA) ist.

Im Jahr 2015 kaufte die Schweizer Armee 6 Hermes-Drohnen von der israelischen Firma Elbit, die nach Angaben der Behörden zu einem der wichtigsten Hersteller von "felderprobten" Drohnen geworden war. Im Jahr 2021 wandte sich die Regierung erneut an Elbit, betreffend einen Auftrag für die Telekommunikation der Armee. Mehrere Stimmen sprachen sich gegen diese Entscheidung aus, insbesondere wegen des Risikos einer Blackbox in der Software, die es einem Drittland ermöglichen könnte, auf sensible Informationen zuzugreifen. Die Behörden vertraten erneut die Auffassung, dass diese Wahl angemessen war, da Elbit das erfolgreichste Unternehmen im Bereich der Telekommunikation sei. Am 11. August berichtete RTS, dass die Eidgenossenschaft so genannte "Regierungssoftware" und versteckte Antennen einsetzt, um Mobiltelefone auszuspionieren oder zu orten (IMSI-Catcher), wenn es um "extrem schwere Verbrechen wie Mord, Vergewaltigung und Unterstützung terroristischer Organisationen" geht. Die NZZ versicherte, es handle sich um die Pegasus-Software(8). NSO ist definitiv eine Kraft, mit der man auf dem Gebiet der Cyber-Überwachung und Cyber-Spionage rechnen muss.

Die Geschichte in der Schweiz hat uns gelehrt, dass der Begriff "terroristische Organisation" vielfältig interpretiert werden kann. Im Jahr 1989 deckte eine parlamentarische Untersuchung die "Fichenaffäre" auf: 900.000 Personen, darunter linksextreme Aktivist*innen, gewählte Politiker*innen usw., wurden von der Bundespolizei völlig ungestraft überwacht und fichiert. Heute wird BDS, eine Bewegung, die die legitimen Rechte der palästinensischen Bevölkerung mit gewaltfreien Mitteln verteidigt, von SVP-Parlamentarier*innen beschuldigt, terroristische Bewegungen zu unterstützen. Werden Aktivist*innen der Extinction Rebellion, die sich für den Einsatz gewaltfreier Mittel zur Sensibilisierung für die Klimakatastrophe einsetzen, von der Justiz ebenfalls als Extremistinnen eingestuft?

Der weit verbreitete Einsatz von Überwachungs- und Spionagesoftware durch Schurkenstaaten, aber auch durch Regierungen in so genannten demokratischen Ländern, stellt eine große Gefahr dar. Oppositionelle werden in den Augen der Machthaber zu mutmaßlichen Terrorist*innen. Demokratische Rechte - Meinungsfreiheit, Demonstrationsfreiheit - werden zunehmend ausgehöhlt.

Natürlich ist Israel nicht das einzige Land, das Waffen, Überwachungsausrüstung und Software für Cybersicherheit und Spionage produziert und exportiert. Aber es ist das einzige Land im 21. Jahrhundert, das anerkanntermaßen eine Politik der Apartheid betreibt. Nach dem humanitären Völkerrecht ist die Apartheid ein Verbrechen gegen die Menschlichkeit. Im 20. Jahrhundert galt die Apartheid in Südafrika als inakzeptabel. Die Apartheid ist auch im 21. Jahrhundert in Israel/Palästina inakzeptabel. Israelische schwere Waffen, Überwachungs- und Cyberspionage-Waffen sind in erster Linie gegen die palästinensische Bevölkerung gerichtet: Sie dienen dazu, sie von ihrem Land zu vertreiben, sie zu unterwerfen und zu kontrollieren. Durch den Verkauf dieser Waffen in die ganze Welt exportiert der Staat Israel auch seine Unterdrückungsstrategien, seinen Rassismus, seine Überwachungs- und Kontrollstrategien, die dann dazu benutzt werden, all diejenigen zu verfolgen, die gegen Kolonialismus,

Rassismus, die Militarisierung der Gesellschaft und die Ausbeutung der schwächsten Menschen in unseren Gesellschaften kämpfen. Elbit-Drohnen spüren in Zusammenarbeit mit Frontex Flüchtlinge im Mittelmeer auf. Die Strategien der israelischen Armee zur Kontrolle der Palästinenser*innen werden von einigen US-Polizeikräften übernommen. In Indonesien erfasst die NSO-Software LGBTQI+ Menschen.

Aus all diesen Gründen ruft BDS zu einem militärischen Embargo gegen Israel auf. Es geht nicht nur darum, einen Beitrag zum Kampf gegen diesen Schurkenstaat zu leisten, sondern auch darum, sich den weltweiten Kämpfen für Freiheit, Gleichheit und Gerechtigkeit anzuschließen und sie zu stärken.

1. https://forbiddenstories.org

2. https://www.nzz.ch/technologie/pegasus-die-schweiz-hat-umstrittene-spionagesoftware-eingesetzt-ld.1640310?reduced=true

3. https://bds-info.ch/index.php/fr/articles/la-cooperation-de-grandes-universites-israeliennes-avec-les-organes-securitaires

4. https://www.haaretz.com/israel-news/.premium-hebrew-university-to-host-israeli-army-base-on-campus-1.7113981

5. https://www.bankinfosecurity.cm/investments-i-israels-cybersecurity-sector-grow-a-15956

6. https://www.haaretz.com/israel-news/.premium-mysterious-uae-cyber-firm-luring-ex-israeli-intel-officers-with-astronomical-salaries-1.7991274?v=1629128028083

7. https://www.rts.ch/info/suisse/12411718-la-suisse-utilise-aussi-un-logiciel-espion-israelien-du-type-pegasus.html

8. https://www.nzz.ch/technologie/pegasus-die-schweiz-hat-umstrittene-spionagesoftware-eingesetzt-ld.1640310?reduced=true