Fakten über die israelische Cyber-Industrie

30.09.2022

Categories: Apartheid und Siedlungskolonialismus, Überwachungstechnologie

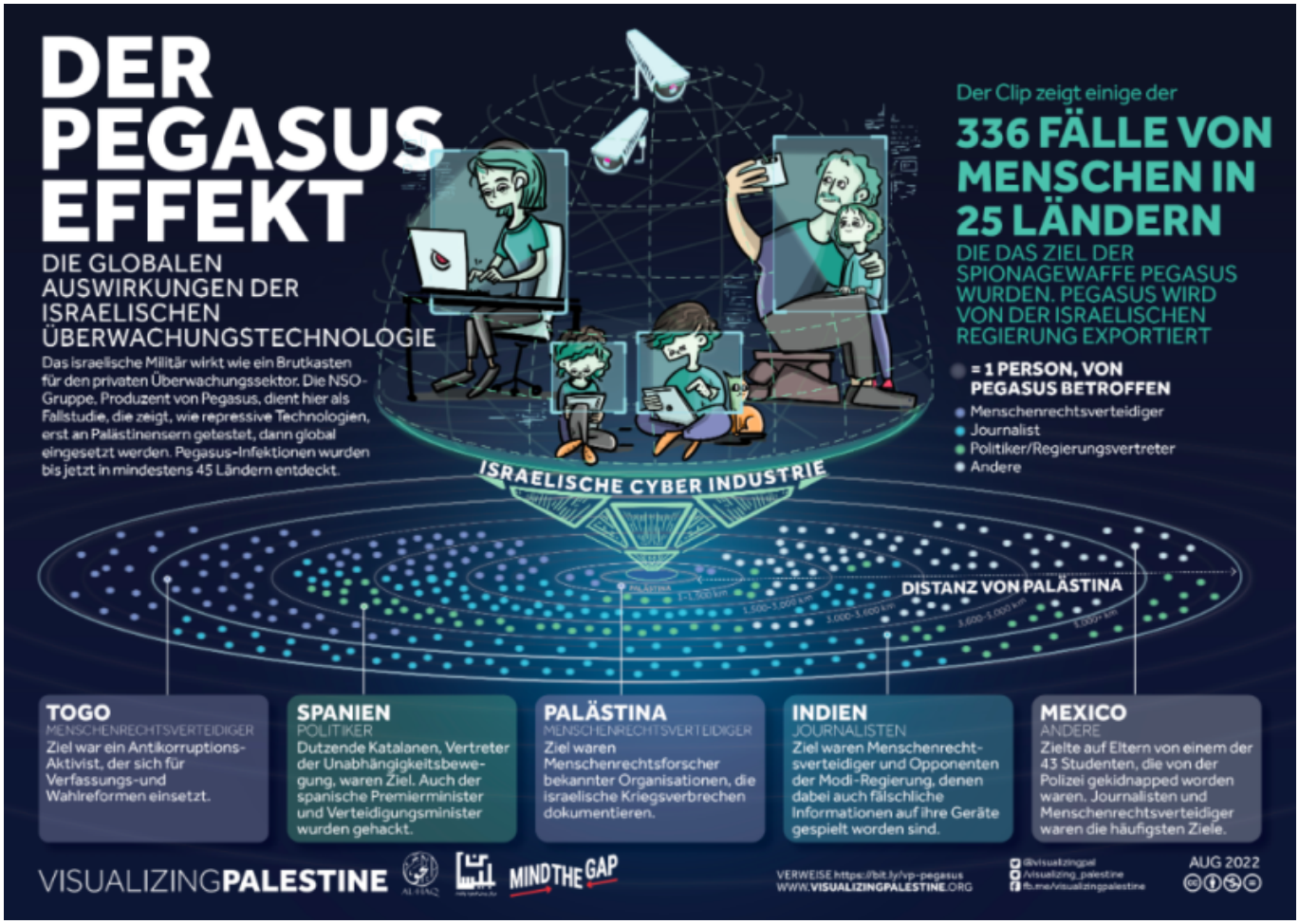
"Das besetzte Palästina fungiert für Israel als Freiluftlabor, in dem Spionage- und Überwachungstechniken getestet werden, bevor diese an repressive Regime in aller Welt verkauft werden.“ – Middle East Institute

"Israels Gebrauch von Überwachungs- und Gesichtserkennungssystemen scheint einer der aufwändigsten Einsätze einer solchen Technologie durch ein Land zu sein, das versucht, eine unterworfene Bevölkerung zu kontrollieren.“ - *AccessNow*

Die Strukturen von israelischem Siedlerkolonialismus, militärischer Besatzung und Apartheid haben es Israel ermöglicht, eine der größten Cyberindustrien der Welt aufzubauen. Durch den Export von Technologien wie dem Pegasus-Spionageprogramm exportieren die israelische Regierung und private israelische Unternehmen das Knowhow, das sie sich bei der Massenüberwachung von Palästinenser*innen und der staatlichen Gewalt seitens des Apartheidregimes aneignen. Sie profitieren von der wachsenden Nachfrage derer, die weltweit Menschenrechtsverteidiger*innen, Journalist*innen und politische Gegner*innen bedrohen.

Die palästinensische Zivilgesellschaft ruft zum Verbot des Handels mit Cyber-Überwachungstechnologien auf, zu denen nicht nur die Spionagesoftware Pegasus, sondern auch biometrische Überwachungstechnologien gehören, die aus der Distanz Massenüberwachung ermöglichen.

Visualizing Palestine hat in Ergänzung zum Bildmaterial **"Der Pegasus Effekt: Die globalen Auswirkungen der israelischen Überwachungstechnologie"**, das in Zusammenarbeit mit Al Haq, dem Bisan Center und dem Mind the Gap Consortium erstellt wurde, nachfolgende Fakten zusammengestellt:



Dieses Bildmaterial ansehen und herunterladen: https://visualizingpalestine.org/visuals/the-pegasus-effect

ISRAELS CYBER-INDUSTRIE

- Israel hat mehr Überwachungsfirmen pro Kopf als jedes andere Land;
- 2020 fielen 31% aller weltweit getätigten Cyberinvestitionen auf israelische Unternehmen
- Israelische Cyber-Unternehmen exportieren sowohl offensive als auch defensive Cyber-Technologien und profitieren davon, dass sie sowohl die raffiniertesten Bedrohungen als auch Technologie gegen diese Bedrohungen anbieten können.
- Für 2020 werden Israels gesamte Militärexporte auf 8,8 Milliarden Dollar und die Cyber-Exporte auf 10 Milliarden Dollar geschätzt.
- Die israelische Regierung betreibt „Spyware-Diplomatie“ und setzt offensive Cyber-Technologie als Faustpfand in Verhandlungen ein, um die Normalisierung in Ländern wie Bahrain, den Vereinigten Arabischen Emiraten, Marokko und Saudi-Arabien voranzubringen.

UNIT 8200

- Die Einheit 8200, die für die israelische Cyber-Offensive zuständige Geheimdiensteinheit, ist die größte Einheit des israelischen Militärs.
- Einheit 8200 fungiert als Talentschmiede für private israelische Cyber- und Tech-Unternehmen, deren Abgänger*innen über 1000 Unternehmen gegründet haben.
- Von den 2300 Israelis, die eine der 700 israelischen Cyber-Firmen gegründet haben, waren 80 % Absolvent*innen der Einheit 8200. Diese Gründer*innen nutzen ihre militärische Erfahrung und

Verbindungen als Marketinginstrument gegenüber ausländischen Investor*innen.
- Die von der Einheit 8200 gesammelten Informationen werden „zur politischen Verfolgung und zur Spaltung der palästinensischen Gesellschaft verwendet“.

ISRAELISCHE UNIVERSITÄTEN

Zwischen israelischen Hochschulen, dem israelischen Militär und israelischen Cyber-Unternehmen gibt es einen engen Austausch:

- Sechs israelische Universitäten haben Zentren, die sich mit Cyber-Forschung befassen.
- Israelische Universitäten führen militärische Forschung durch, die von der Forschungs- und Entwicklungsabteilung des israelischen Verteidigungsministeriums (DDR&D) und von Militärunternehmen geleitet wird.
- Israelische Universitäten bieten Programme für das israelische Militär und den militärischen Nachrichtendienst an, darunter das Academic Reserves-Programm (Atuda), das Talpiot- und das Havatzalot-Programm.

Massenüberwachung der Palästinenser*innen

Israels weit verbreiteter Einsatz von Massenüberwachung und gezielter Spionagesoftware stützt sein Apartheidregime und die systematische Verweigerung zahlreicher Grundrechte wie das Recht auf Privatsphäre, Freizügigkeit, Diskriminierungsfreiheit, Meinungs- und Vereinigungsfreiheit, ordnungsgemässe Gerichtsverfahren und vieles mehr.

- Die Massenüberwachung gibt Israel die unkontrollierte Macht, Informationen über Palästinenser*innen zu sammeln, die vor Militärgerichten mit einer fast 100-prozentigen Verurteilungsquote angeklagt werden, oft auf der Grundlage „geheimer Beweise“.
- Israelische Soldat*innen fotografieren Palästinenser*innen an Checkpoints, um eine bevölkerungsweite Datenbank für Blue Wolf, ein Smartphone-basiertes Gesichtserkennungsprogramm, aufzubauen.
- Israel nutzt Netzwerke von CCTV-Kameras, ausgestattet mit biometrischen Funktionen, um Palästinenser*innen in Städten wie Hebron, Jerusalem und im gesamten Westjordanland in Echtzeit zu überwachen.
- Israel ist in der Lage, jeden Telefonanruf in der Westbank und Gaza zu überwachen und abzuhören.
- Palästinensische Menschenrechtsverteidiger*innen, die für Organisationen arbeiten, die von der israelischen Regierung attackiert werden, sind Zielscheibe der Spionagesoftware Pegasus, der derzeit raffiniertesten offensiven Cyberwaffe.
- „Die palästinensische Bevölkerung unter militärischer Besatzung ist der Spionage und Überwachung durch israelische Geheimdienste völlig ausgeliefert.“ (Unit 8200-Reservisten)

DIE NSO-GRUPPE UND DIE PEGASUS-SPIONAGESOFTWARE

- Die NSO-Gruppe, ein israelisches Cyber-Unternehmen, das 2010 gegründet wurde, ist Entwickler der Pegasus-Spionagesoftware.
- Pegasus ist fähig zu Zero-Click-Infektionen, das heisst, das Spionageprogramm kann vollständigen

Zugriff auf das Smartphone oder das Gerät einer Zielperson erlangen und alle Daten herunterladen, ohne dass die Person auf einen Malware-Link klicken muss.
- Die NSO-Gruppe hat Pegasus an Regierungen verkauft, die schwere Menschenrechtsverletzungen begehen.
- Jeder Verkauf von Pegasus wird von der israelischen Behörde für die Kontrolle von Verteidigungsexporten genehmigt. Informationen über diese Ausfuhrgenehmigungen werden nicht einmal gegenüber der israelischen Knesset freigegeben.
- Wissenschaftler*innen und Journalist*innen haben bestätigt, dass Pegasus in grossem Umfang eingesetzt wird, um Journalist*innen, Menschenrechtsaktivist*innen und Politiker*innen ins Visier zu nehmen. Sie haben Beweise gefunden, dass das Spionageprogramm in mindestens 45 Ländern eingesetzt wird.
- 50 000 Telefonnummern einschliesslich derjenigen von Menschenrechtsverteidiger*innen, Journalist*innen und Politiker*innen erscheinen auf einer geheimen Liste potenzieller Zielpersonen für Pegasus, die der NSO-Gruppe zur Verfügung gestellt wurde.
- Pegasus ermöglicht die grenzüberschreitende Überwachung, beispielsweise wurden Angehörige des ermordeten Journalisten Jamal Khashoggi überwacht. Mit Pegasus können Staaten Menschenrechtsverletzungen auch über ihr eigenes Staatsgebiet hinaus begehen.
- Pegasus wird mit Fällen in Verbindung gebracht, wo staatliche Behörden Beweise manipulieren, um Dissidenten zu belasten, wie etwa im Fall von Bhima Koregaon in Indien.
- Gegen die NSO-Gruppe sind von Whatsapp, von Apple und in Frankreich vom palästinensischen Aktivisten und Rechtsanwalt Salah Hammouri Klagen eingereicht worden.

PEGASUS UND DIE US-POLITIK

- Im November 2021 verbot das US-amerikanische Handelsministerium den Handel mit der NSO-Gruppe, weil dasUnternehmen „Spionagesoftware entwickelt und ausländischen Regierungen zur Verfügung gestellt hat, die dieses Programm benutzt haben, um sie in böswilliger Absicht gegen Regierungsvertreter*innen, Journalist*innen, Geschäftsleute, Akademiker*innen und Botschaftsangehörige einzusetzen“.
- Vor dem Verbot erwarb das FBI Pegasus zur Inlandsüberwachung und die CIA stellte Pegasus der Regierung von Dschibuti zur Verfügung.
- Seit dem Verbot hat Berichten zufolge das US-Verteidigungsunternehmen L3Harris im Juni 2022 Gespräche mit der NSO-Gruppe geführt, um Pegasus zu kaufen.
- Gemäss einer Recherche von DAWN haben US-Lobbyisten der NSO-Gruppe gegen das Gesetz zur Registrierung ausländischer Agenten verstossen, „indem sie die Verbindungen zwischen dem israelischen Spionage-Unternehmen und der Regierung von Israel falsch darstellten“.

Quelle : Visualizing Palestine

WEITERE LITERATUR

1. **“**The Pegasus Project: Global Democracy Under Cyber Attack**,” Amnesty International**
2. “**The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights**,” 7amleh
3. “**Israeli Spyware Facilitates Human Rights Violations Globally on a Massive Scale**,” BDS Global Campaign

4. “**Repression Diplomacy: The Israeli Cyber Industry**,” Who Profits
5. “**Digital Violence: How the NSO Group Enables State Violence**,” Forensic Architecture
6. “**Six Palestinian Human Rights Defenders Hacked with NSO Group’s Pegasus Spyware**,” Frontline Defenders
7. “**Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries**,” Citizen Lab
8. “**Operating from the Shadows: Inside NSO Group’s Corporate Structure**,” SOMO, Privacy International, Amnesty International