

Pegasus Software und Corona-Maßnahmen befördern Überwachungsstaat

Annette Groth, November 2021

Dass Corona seit langer Zeit das beherrschende Thema in unseren Mainstreammedien ist, dürfte der politischen Elite sicherlich sehr gelegen sein. Neben vielen anderen Themen wird über die alltäglichen Menschenrechtsverletzungen in Palästina, die Vertreibung der Palästinenser:innen aus ihren Häusern und von ihren Ländereien sowie die Gewaltexzesse gegen die Bevölkerung kaum berichtet.

Was wäre das für ein Aufschrei gewesen, wenn Putin international bekannte Menschenrechtsorganisationen, mit denen der Westen zusammenarbeitet, als Terrororganisationen eingestuft hätte! Die Forderungen nach den schlimmsten Sanktionen und Boykottaufrufen wären noch das Mindeste vonseiten der europäischen Regierungen und zivilgesellschaftlichen Organisationen gewesen, angesichts der allgegenwärtigen Russlandhetze ist auch Schlimmeres vorstellbar.

Im Oktober hat es der israelische Verteidigungsminister Benny Gantz gewagt, sechs international bekannte palästinensische Menschenrechtsorganisationen als „Terrororganisationen“ zu bezeichnen. Harsche Kritik kam von etlichen Menschenrechtsorganisationen im In- und Ausland wie auch von einigen Politikern, aber der große Aufschrei blieb aus. Dabei wäre dieser absolut nötig, weil auch die Finanzierung dieser Menschenrechtsorganisationen durch deutsche und internationale Organisationen wie Medico, Brot für die Welt, Misereor und anderen gestoppt würde, wenn die Kategorisierung als „Terrororganisation“ aufrechterhalten würde.

Warum? Nach Artikel 24a des israelischen „Terrorbekämpfungsgesetzes“ aus dem Jahr 2016 wird jede Person, die sich mit einer Terrororganisation solidarisiert – auch durch die Veröffentlichung von Lob, Unterstützung oder Ermutigung – mit drei Jahren Gefängnis bestraft. Dies gilt für die Mitarbeiter der sechs palästinensischen Organisationen und für alle weiteren in Israel und außerhalb Israels, die sich mit ihnen solidarisch erklären.

Der israelische Verteidigungsminister gab als Grund für die Bezeichnung „Terrororganisationen“ an, dass diese Organisationen mit der Volksfront für die Befreiung Palästinas (PFLP) zusammenarbeiten würden, wobei ein Beweis für diese Behauptung fehlt.

Menschenrechtsorganisationen werden von der Spionagesoftware Pegasus ausspioniert

Die sechs Menschenrechtsorganisationen wurden von der Spionagesoftware Pegasus der israelischen NSO Group überwacht. Auf den Handys mehrerer Mitglieder wurden Spuren des Pegasus-Trojaners gefunden. Gegenüber der New York Times bestritten das Büro des israelischen Premierministers und das Verteidigungsministerium, die Pegasus-Software eingesetzt zu haben.

Die Software ermöglicht Zugriffe auf Kamera und Mikrofon eines Handys und kann den Standort, Kalendereinträge und Adressen abfragen. „Da die Software direkt „im Handy“ und damit an der „Quelle“ sitzt, können auch Nachrichten, die über Messenger-Apps mit Ende-zu-Ende Verschlüsselung

versendet werden, noch vor der Verschlüsselung im Klartext abgefangen und ausgelesen werden. Das ermöglicht ein „live“ mitlesen“. (1)

Bereits im Juli dieses Jahres hatte ein internationales Pegasus-Recherche-Projekt von mehr als 80 Medienschaffenden in zehn Ländern (u.a. Süddeutsche Zeitung, NDR, WDR, Die Zeit, Guardian, Washington Post) enthüllt, wie Staaten die NSO-Spähsoftware weltweit gegen Menschenrechtler:innen, Journalist:innen und Oppositionelle einsetzen. So wird auch der Mord an Jamal Ahmad Khashoggi im saudi-arabischen Konsulat in Istanbul mit NSO in Verbindung gebracht. Amnesty International erhielt im Juli eine Liste, auf der über 50.000 Zielpersonen der NSO Group stehen sollen. Darunter befinden sich neben dem französischen Regierungschef Emmanuel Macron auch der Präsident des Europäischen Rates Charles Michelle. (2)

Obwohl die Spionagesoftware heftig kritisiert wird und neben Amnesty International viele Organisationen einen internationalen Exportstopp für die Überwachungssoftware der Firma NSO fordern, hat auch das Bundeskriminalamt (BKA) die Spähsoftware Pegasus erworben und nutzt sie seit diesem Jahr für das Ausspionieren von Verdächtigen. Laut BKA werden in „einer mittleren einstelligen Zahl von Ermittlungsverfahren Personen mithilfe von Pegasus überwacht.“ (3) Im Oktober wurde bekannt, dass auch der Bundesnachrichtendienst (BND) Pegasus einsetzt, um damit im Ausland zu spionieren.

Besonders brisant an dieser Überwachungsmethode ist, dass die Kunden, also auch BKA und BND, die Software nicht autonom bedienen können. Sie sind auf die Mithilfe der NSO Group angewiesen und liefern diesen die zur Durchführung der jeweiligen Abhörmaßnahmen notwendigen Informationen (bspw. die zu überwachende Telefonnummer). D.h. alle staatlichen Behörden und Geheimdienste, die Pegasus benutzen, können das nur in Kooperation mit der israelischen Firma NSO, die damit über alle Einsätze ihrer Überwachungssoftware informiert ist! Schon allein diese Tatsache müsste ausreichen, dem BKA und BND die Nutzung zu verbieten, da die Weitergabe von durch Pegasus gesammelten Informationen möglich ist und dies einen gravierenden Verstoß gegen das Datenschutzgesetz und die Sicherheitsinteressen der Bundesrepublik darstellt.

USA sanktionieren Pegasus-Software

Die USA scheinen die Gefahr der Software erkannt zu haben und setzten Anfang November 2021 die Pegasus-Software und eine weitere israelische Softwarefirma namens Candiru auf die „Entity List“. Auf der "Entity List" führt die US-Regierung Unternehmen, Personen oder Regierungen, deren Aktivitäten "den nationalen Sicherheits- oder außenpolitischen Interessen der Vereinigten Staaten zuwiderlaufen". Der Handel mit diesen unterliegt strengen Beschränkungen und ist teilweise nur mit einer Ausnahmegenehmigung des Ministeriums erlaubt.

Im Mai 2019 hatte die US-Regierung unter Präsident Donald Trump Huawei auf diese Liste gesetzt, mit weitreichenden Folgen für das chinesische Unternehmen und seine zahlreichen US-Handelspartner. Huawei kann wegen der Beschränkungen unter anderem keine Smartphones mit Googles

Android mehr anbieten und musste sich infolge von einem großen Teil seines Smartphone-Geschäfts trennen.

Als Begründung für die Strafmaßnahme gegen die NSO Group und Candiru wurde angegeben, dass diese Unternehmen "Spionagesoftware entwickelt und an ausländische Regierungen geliefert haben". Die Software sei zur "Überwachung von Regierungsbeamten, Journalisten, Geschäftsleuten, Aktivisten, Wissenschaftlern und Botschaftsmitarbeitern eingesetzt" worden. (4) NSO hat diese Vorwürfe zurückgewiesen und betont, dass ihre Kunden ausschließlich staatliche Behörden sind. Das darf stark bezweifelt werden.

Ermutigt von der Strafmaßnahme der US-Regierung dürfte Apple dazu gebracht haben, kürzlich gegen das Unternehmen Strafanzeige einzureichen. Der US-Konzern will gerichtlich ein Nutzungsverbot aller Apple Geräte und Software durch die NSO Group erstreiten. In der Klage wird auch eine „Wiedergutmachung“ für das Ausspähen von Nutzern gefordert, weil dies gegen US-Recht verstoßen habe.

Wie die israelische Zeitung Haaretz am 23.11. 2021 meldete, stehen die Firma NSO Group und das Unternehmen Candiru aufgrund der eingeleiteten Strafmaßnahme und Klagen vor der Zahlungsunfähigkeit. (5)

Angesichts dieser Entwicklung und der überaus großen Gefahr, die von der Spionagesoftware ausgeht, sollten die Bundesregierung und die EU-Mitgliedsstaaten dem US-Beispiel folgen und ihren Einsatz verbieten.

BDS-Kampagne fordert Verbot

Das Nationale Komitee der palästinensischen BDS-Kampagne (Boykott, Desinvestitionen und Sanktionen) hat auf die Veröffentlichung von Amnesty International schnell reagiert und den Aufruf „Vereint gegen Cyber-Überwachung und Repression“ gestartet und ein Verbot der Cyber-Überwachung gefordert.

In ihrem Aufruf analysiert das Komitee die israelische Militär-, Sicherheits- und Überwachungstechnologie, die „die Grundlage für Israels Beziehungen zum Rest der Welt“ bildet.

„Das israelische Militär hat in Zusammenarbeit mit seinen Universitäten und Forschungszentren nicht nur die Technologie und Methodik entwickelt, die zur Unterwerfung und Unterdrückung der Palästinenser eingesetzt werden. Es hat auch ein ausgeklügeltes System eingerichtet, das seine "felderprobte" Militär- und Massenüberwachungstechnologie auf den profitablen globalen Markt der Überwachungsindustrie lenkt. Es hat seine militärische Geheimdienst Einheit 8200 in einen Startup-Inkubator umgewandelt und wirbt aggressiv für seine Kapazitäten...“ (6)

Israel beheimatet die höchstentwickelste Überwachungs-Industrie der Welt mit einer großen Expertise nicht nur bei der Sammlung und Verarbeitung von Daten, bei der Gesichtserkennung, sondern auch bei den „Tools zur Benutzerverfolgung“, die für polizeiliche Zwecke, Wahlmanipulationen und mehr eingesetzt werden können.

Durch die illegale Dauer-Besetzung der Westbank und des Gaza-Streifens ist Israel auch das perfekte Digital-Labor für die Bekämpfung von Aufständen und die Kontrolle von Menschen.

Die jungen Soldaten und Soldatinnen der israelischen Armee „erhalten in den riesigen Entwicklungsabteilungen, die das Militär gegründet hat, alle Freiheiten, um in der digitalen Welt an der Spitze zu sein“; so der israelische Autor Ronen Bergman über seine mehrjährige Recherchearbeit in der israelischen Digitalindustrie. (7)

Das Militär ist der Motor und Innovationstreiber für die mehr als 5.000 Start-ups, die gern von US- und anderen Westkonzernen gekauft werden. Häufig werden die Firmen von Ex-Offizieren der israelischen Armee gegründet, die „ihre Erfahrungen bei der Fern- und Nah-Erkennung, Bekämpfung und Tötung von Palästinensern in „ziviler“ unternehmerischer Form“ nutzen. (8) So war auch der NSO-Mitbegründer Shalev Hulio mit der israelischen Armee gegen die Zweite Intifada im Westjordanland eingesetzt.

Künstliche Intelligenz spielt in der Waffenindustrie eine immer größere Rolle und sollte angesichts der drohenden Bewaffnung der Drohnen, wie sie die neue Ampel-Regierung anvisiert, intensiv debattiert werden. Um die Bewaffnung zu verhindern, haben kürzlich zahlreiche Forscher:innen der Künstlichen Intelligenz und Informatik einen öffentlichen Appell an die Ampel Parteien lanciert:

Die Bewaffnung von Drohnen für die Bundeswehr stoppen – autonome Waffensysteme ächten!

In dem Appell heißt es:

„Die Bewaffnung von Drohnen macht eine autonome Waffenführung prinzipiell möglich und stellt einen kritischen Wendepunkt dar. Die Revolution in der Künstlichen Intelligenz hat eine algorithmen-gesteuerte Kriegsführung in absehbarer Zukunft möglich gemacht. Bisher gibt es jedoch keine nationalen oder internationalen Kontrollregime, die dieser bereits stattfindenden Entwicklung Einhalt gebieten.

Bereits der Einsatz von vom Menschen gesteuerten bewaffneten Drohnen hat die Schwelle zum Einsatz militärischer Gewalt gesenkt und den Krieg weiter entgrenzt, Drohnenangriffe finden dauerhaft und häufig ohne Kriegserklärung statt.

Die zunehmende Automatisierung von bewaffneten Drohnen verschärft gleichzeitig die Gefahr einer militärischen Konfrontation zwischen Staaten, die mit solchen Waffen ausgerüstet sind. Wird aufgrund eines realen militärischen Zwischenfalls oder eines Fehlalarms ein autonomes Waffensystem aktiviert, wird sich eine militärische Eskalation nicht mehr aufhalten lassen. Damit droht eine Verschärfung globaler Instabilität. Diese Szenarien sind keine ferne Dystopie – im Juni diesen Jahres haben die Vereinten Nationen in einem Bericht bekannt gegeben, dass in Libyen vermutlich eine Drohne einen vollautonomen Angriff durchgeführt hat.

Angesichts der rasanten Entwicklung der Künstlichen Intelligenz ist die Entwicklung und Verbreitung von modernen bewaffneten Drohnen der Dambruch für einen globalen Rüstungswettlauf hin zu autonomer Kriegsführung, der jetzt gestoppt werden kann und muss“. (9)

Es ist zu hoffen, dass dieser Appell gehört und auch befolgt wird!

Angesichts des Säbelrasselns und der Drohungen gegen China und Russland ist die Gefahr eines „Krieges aus Versehen“ bereits sehr groß und wird durch Künstliche Intelligenz und autonome Waffensysteme noch größer.

Aufgrund ihrer Gefährlichkeit sollten diese neuen Technologien viel mehr Aufmerksamkeit bekommen und breit diskutiert werden. Sie sind ein bedeutender Faktor für die zunehmende Aushöhlung der Bürgerrechte.

- (1) <https://www.lto.de/recht/hintergruende/h/spysoftware-pegasus-bka-einsatz/>
- (2) <https://www.amnesty.ch/de/themen/ueberwachung/dok/2021/projekt-pegasus-spionage-gegen-zivilgesellschaft>
- (3) <https://www.lto.de/recht/hintergruende/h/spysoftware-pegasus-bka-einsatz/>
- (4) <https://www.heise.de/news/Spyware-Pegasus-USA-verhaengen-Sanktionen-gegen-NSO-Group-und-andere-6250364.html>
- (5) <https://www.haaretz.com/israel-news/tech-news/israeli-spyware-firm-nso-at-risk-of-defaulting-after-u-s-blacklisting-1.10408897>
- (6) <http://bds-kampagne.de/2021/07/22/ein-aufruf-aus-palaestina-vereint-gegen-cyber-ueberwachung-und-unterdrueckung/>
- (7) Ronen Bergman. Der Geheimdienst-Experte über Israels Spione, ihre gezielten Tötungen und den gescheiterten Atomdeal mit dem Iran, Handelsblatt 11.5.2018
- (8) <https://www.nachdenkseiten.de/?p=74434> 20.7.2021: Lauschangriff mit israelischer Besatzungs-Technologie, Werner Rügemer
- (9) <https://aiscientists4peace.org>