Deutscher Bundestag **Drucksache 20/19**

20. Wahlperiode 09.11.2021

Kleine Anfrage

der Abgeordneten Martina Renner, Jan Korte, Nicole Gohlke, Anke Domscheit-Berg, Dr. André Hahn, Andrej Hunko, Ina Latendorf, Ralph Lenkert, Dr. Gesine Lötzsch, Żaklin Nastić, Petra Pau, Victor Perli, Dr. Petra Sitte, Kathrin Vogler und der Fraktion DIE LINKE.

Einsatz von Produkten der Firma NSO Group Technologies durch deutsche Sicherheitsbehörden

Im Juli dieses Jahres wurde bekannt, dass weltweit Journalisten, Menschenrechtsaktivistinnen, Geschäftsleute und Regierungspolitiker Opfer von Überwachungsmaßnahmen mithilfe des Programms „Pegasus“ der u. a. in Israel beheimateten Firma „NSO Group Technologies“ geworden waren (vgl. die Vorbemerkung der Fragesteller in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/32246). Durch den Einsatz der Software ist es möglich, selbst verschlüsselte Kommunikation zu überwachen.

Auch der Deutsche Bundestag beschäftigte sich daraufhin mit diesem Vorgang und der Frage des Einsatzes von „Pegasus“ durch deutsche Behörden, unter anderem in einer Sondersitzung des Ausschusses für Inneres und Heimat am 7. September 2021. Nachdem von der Bundesregierung zunächst jede Antwort zu Fragen betreffend den Einsatz durch deutsche Behörden mit Verweis auf eine vermeintliche Gefährdung das „Staatswohls“ verweigert worden war, musste sie in dieser Sitzung nach Medienberichten den Gebrauch durch das Bundeskriminalamt (BKA) einräumen (tagesschau.de vom 7. September 2021, „BKA soll Seehofer nicht informiert haben“). Demnach soll eine „modifizierte Version der Spionagesoftware“ vom BKA auch in Deutschland eingesetzt werden. Bei der Modifikation ging es demnach um eine Anpassung an die deutsche Rechtslage, weil der Leistungsumfang der ursprünglich angebotenen Software das rechtlich Zulässige überschritten habe. Es sei sichergestellt worden, dass keine sensiblen Daten an die NSO Group hätten abfließen können, und es hätte eine vertragliche Zusicherung gegeben, dass die erfassten Daten nicht an Dritte weitergegeben werden. Technisch kann dies nach Ansicht der fragestellenden Fraktion jedoch nicht sichergestellt werden, solange die Installation des Programms, Server zur Steuerung und zur Entgegennahme der ausgeleiteten Daten und die Übermittlung an die Auswertung in den zuständigen Behörden nicht vollständig durch diese Behörden vorgenommen bzw. betrieben werden. Insofern besteht Unklarheit, ob diese Voraussetzungen erfüllt sind.

Einer Meldung in der „ZEIT“ zufolge (Bundesnachrichtendienst setzt umstrittene Cyberwaffe ein, ZEIT ONLINE vom 8. Oktober 2021) hat auch der Bundesnachrichtendienst „Pegasus“ eingesetzt, „dem Vernehmen nach“ mit Kenntnis und Billigung des Bundeskanzleramtes.

Wir fragen die Bundesregierung:

1. Hat die Bundesregierung mittlerweile alle ggf. infrage kommenden Gremien des Deutschen Bundestages über den Einsatz der Spionagesoftware „Pegasus“ durch Behörden im Zuständigkeitsbereich dieser Gremien unterrichtet?

   Wenn nein, warum ist eine solche Unterrichtung bislang unterblieben?

2. Trifft es zu, dass auf eine technische Prüfung von „Pegasus“ durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) anders als bei früher beschafften oder selbst entwickelten Instrumenten zur informationstechnischen Überwachung verzichtet wurde?

   Wenn ja, warum wurde auf eine solche Prüfung verzichtet?

3. Treffen Presseberichte zu, nach denen das BKA selbst eine informationstechnische Sicherheitsprüfung der Software vorgenommen und an das Bundesamt für Sicherheit in der Informationstechnik übermittelt hat?

   a) Welchen Stellen, Gremien etc. der Bundesregierung oder ihrer nachgeordneten Behörden lag dieser Bericht vor?

   b) Wurde der Bericht parlamentarischen Gremien vorgelegt, wenn ja, welchen, wenn nein, warum nicht?

4. Wurde der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an irgendeiner Stelle des Beschaffungsvorhabens oder nach der Beschaffung zur Software und zu ihrem Einsatz konsultiert und ihm Gelegenheit zur Stellungnahme gegeben?

5. Nach welchen Kriterien, Schemata, fachlichen Vorgaben oder Fragestellungen wurde ggf. eine Überprüfung der Spähsoftware „Pegasus“ durch die einsetzenden Behörden selbst vorgenommen?

6. Hat jede einsetzende Behörde selbst eine solche Überprüfung vorgenommen, und wussten die jeweiligen Behörden von der Beschaffung und dem Einsatz in den anderen Behörden des Bundes?

7. Welche Behörden oder Einrichtungen wurden anlässlich bzw. im Nachgang eigener Überprüfungen der einsetzenden Behörden über die Ergebnisse dieser Überprüfungen unterrichtet?

8. Hat sich infolge von Überprüfungen bzw. Auswertungen des Einsatzes ergeben, dass die dem BKA zur Verfügung gestellte Programmversion von „Pegasus“ weiterer Einschränkungen bedarf oder bestimmte Einschränkungen der angepassten Programmversion gegenüber der Standardversion zurückgenommen werden können?

9. Welche Informationen über „Pegasus“ wurden dem Gericht zur Verfügung gestellt, das den Einsatz im Rahmen von Gefahrenabwehrvorgängen oder Strafermittlungen angeordnet hat?

10. In wie vielen Fällen mit wie vielen Betroffenen wurde „Pegasus“ bislang eingesetzt, und

    a) wie viele dieser Vorgänge sind noch laufend,

    b) wie viele dieser Vorgänge sind bereits abgeschlossen,

    c) welches Ziel wurde mit dem jeweiligen Einsatz verfolgt (Gefahrenabwehr, Strafverfolgung)?

11. In wie vielen Fällen erfolgte bislang nach Abschluss der Maßnahme eine Information an Betroffene, in wie vielen Fällen wurde vorläufig von einer Benachrichtigung abgesehen oder soll dauerhaft davon abgesehen werden?

12. Welchen Schweregrad (base score) nach dem Common Vulnerability Scoring System (CVSS) haben die beim Einsatz der modifizierten Version der Spähsoftware „Pegasus“ genutzten Vektoren zur Ausleitung von Daten aus dem jeweiligen Zielsystem, und welche Kosten hat die Beschaffung und Aufrechterhaltung der Fähigkeiten zur Wahrnehmung dieser Befugnisse vor dem Hintergrund der Einführung neuer Betriebssystem-Versionen im Jahr 2021 bisher verursacht?

13. Gibt es nach Ansicht der Bundesregierung ganz generell die Möglichkeit, bei einer durch einen privaten Partner betriebenen technischen Infrastruktur zur Infiltration eines Zielsystems und der anschließenden Ausleitung von Daten aus laufender oder abgeschlossener Kommunikation technisch auszuschließen, dass die ausgeleiteten Daten auch an den Betreiber selbst oder an Dritte ausgeleitet werden oder der Datenstrom gespiegelt wird?

14. Für wie zuverlässig hält die Bundesregierung vertragliche Zusicherungen, keine der erhobenen Daten an Dritte, einschließlich ausländischer staatlicher Stellen, auszuleiten, durch einen Vertragspartner, der in der Vergangenheit durch Zusammenarbeit mit Regimen der saudi-arabischen Halbinsel, Umgehung exportrechtlicher Regulierung durch diverse Holdings in unterschiedlichen Staaten und der Beteiligung an der Ausspähung von Journalistinnen und Menschenrechtsaktivisten von sich reden machte?

15. Welche Erkenntnisse hat die Bundesregierung, beispielsweise aus der Marktsichtung durch die Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) oder Bedarfsträger in ihrem Geschäftsbereich, welche Firmen mit ähnlichen Angeboten wie der NSO Group für staatliche Bedarfsträger derzeit weltweit agieren?

16. Wann und mit welchem Ergebnis hat sich ZITiS insbesondere hinsichtlich des verfassungskonformen Einsatzes mit „Pegasus“ beschäftigt?

17. Wer wurde von ZITiS wann über das Ergebnis dieser Prüfung unterrichtet, und wie hat die zuständige Fach- und Rechtsaufsicht sich zu diesem Prüfergebnis verhalten?

18. Inwieweit wurde ZITiS vom Einsatz von „Pegasus“ in Kenntnis gesetzt oder hat Kenntnis von technischen Fragen und Problemstellungen im Rahmen des Einsatzes (etwa zum Aufbau von Know-how für zukünftige Beschaffungen in diesem Bereich) erhalten?

19. Mit welchen dieser Firmen hatten ZITiS, das BKA, das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst (BND) oder der Zoll im Rahmen von Marktsichtungen Kontakt, und welche dieser Firmen konnten wie die NSO Group (vgl. Antwort der Bundesregierung zu Frage 1 auf Bundestagsdrucksache 19/32246) ihre Produkte bzw. ihr Portfolio präsentieren (bitte soweit möglich mit Firmennamen, Produkten, Behörde bzw. Einrichtung, Datum auflisten)?

20. Inwieweit gab es beim BND eine Prüfung, ob die mit „Pegasus“ erfassten Daten bei einer erlaubten Weitergabe oder einer unerlaubten Ausleitung an Dritte zur Zielerfassung für Drohnenangriffe geeignet sind?

21. Hat der BND die mit „Pegasus“ erfassten Daten und Kommunikationsinhalte mit ausländischen Nachrichtendiensten geteilt, und wenn ja, in welcher Form, und welchem Umfang?

22. Was ist der Bundesregierung zur rechtlichen Regulierung von Firmen wie der NSO Group und anderen, die Software zur informationstechnischen Überwachung anbieten, in Israel bekannt?

23. Was ist der Bundesregierung zum Aufbau dieses Sektors in Israel hinsichtlich direkter oder indirekter staatlicher Finanzhilfen, Start-up-Gründungen aus Behörden und Universitäten heraus und durch weitere wirtschaftspolitische Maßnahmen bekannt?

    Nimmt sich die Bundesregierung diese Maßnahmen zum Vorbild für den Aufbau eines eigenen Wirtschaftssektors im Bereich Cyber-Sicherheit in Deutschland, und wenn ja, welche?

24. Welche Projekte werden derzeit im Rahmen der Tätigkeit der Agentur für Innovationen in der Cyber-Sicherheit und von ZITiS durchgeführt oder unterstützt, und mit welchen privatwirtschaftlichen Partnern arbeiten diese Stellen und Einrichtungen dabei zusammen?

Berlin, den 5. November 2021

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333