Deutscher Bundestag **Drucksache 20/321**

20. Wahlperiode 17.12.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Martina Renner, Jan Korte, Nicole Gohlke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 20/19 –

Einsatz von Produkten der Firma NSO Group Technologies durch deutsche Sicherheitsbehörden

Vorbemerkung der Fragesteller

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.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 17. Dezember 2021 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

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.

Vorbemerkung der Bundesregierung

Die Bundesregierung ist nach sorgfältiger Prüfung unter Abwägung der im Staatswohl begründeten Geheimhaltungsinteressen der Bundesregierung mit dem parlamentarischen Informationsanspruch zu der Einschätzung gelangt, dass eine Beantwortung der Fragen 2, 5, 6, 7 und 11 in Bezug auf das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst und den Militärischen Abschirmdienst, der Fragen 10, 12, 15 und 19 in Bezug auf die Sicherheitsbehörden und Nachrichtendienste des Bundes und der Fragen 20 und 21 in Bezug auf den Bundesnachrichtendienst nicht beziehungsweise nicht vollständig erfolgen kann, da bezüglich der mit diesen Fragen erbetenen Informationen überwiegende Belange des Staatswohls einer (vollständigen) Beantwortung entgegenstehen.

Mit den aus der Beantwortung dieser Fragen ableitbaren Informationen über die den betroffenen Sicherheitsbehörden des Bundes gegebenenfalls zur Verfügung oder nicht zur Verfügung stehenden kriminaltaktischen (Fragen 10, 12, 15 und 19) oder nachrichtendienstlichen (Fragen 2, 5, 6, 7, 10, 11, 12, 15, 19, 20 und 21) Ermittlungs- beziehungsweise Informationsgewinnungsinstrumenten würde die Bundesregierung technische Einzelheiten polizeilicher beziehungsweise nachrichtendienstlicher Ermittlungs-/Analysefähigkeiten und Vorgehensweisen zur Gefahrenabwehr oder zur Verhinderung und Aufklärung von Straftaten offenlegen oder Rückschlüsse darauf ermöglichen. Hierdurch würden die Arbeitsfähigkeit und Aufgabenerfüllung der betroffenen Sicherheits- und Strafverfolgungsbehörden sowie der Nachrichtendienste erheblich gefährdet, weil Täter oder potentielle Zielpersonen ihr Verhalten anpassen und künftige Überwachungs- beziehungsweise Aufklärungsmaßnahmen dadurch erschweren oder gar vereiteln könnten, etwa durch Aktivitäten zur Hinderung des Einsatzes oder zur Umgehung der entsprechenden Instrumente. Bereits Angaben zu Herstellern technischer Produkte im Bereich der informationstechnischen Überwachung, von denen die betroffenen Sicherheitsbehörden des Bundes Gebrauch oder keinen Gebrauch machen, könnten zu einer gezielten Änderung des Kommunikationsverhaltens der betreffenden beobachteten Personen führen, was eine (weitere) Aufklärung der von diesen verfolgten Bestrebungen und Planungen unmöglich machen würde. Eine Preisgabe dieser sensiblen Informationen würde sich somit auf die staatliche Aufgabenwahrnehmung im Gefahrenabwehrbereich, wie auch auf die Durchsetzung des Strafverfolgungsanspruchs des Staates und die nachrichtendienstliche Informationsbeschaffung außerordentlich nachteilig auswirken.

Eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Ermittlungsbeziehungsweise Aufklärungsfähigkeiten im Bereich der Telekommunikations- und informationstechnischen Überwachung für die Aufgabenerfüllung der betroffenen Sicherheitsbehörden beziehungsweise der Nachrichtendienste des Bundes nicht in Betracht. Auch ein geringfügiges Risiko des Bekanntwerdens derart sensibler Informationen kann unter keinen Umständen hingenommen werden. Die angefragten Informationen beschreiben die technischen Fähigkeiten der betroffenen Sicherheitsbehörden beziehungsweise der Nachrichtendienste des Bundes aufgrund ihres Bezuges auf bestimmte Produkte oder Hersteller in einem derartigen Detaillierungsgrad, dass eine Bekanntgabe auch

gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen würde.

Daraus folgt, dass die mit den oben genannten Fragen erbetenen Informationen derartig schutzbedürftige Geheimhaltungsinteressen berühren, dass auch das geringfügige Risiko eines Bekanntwerdens, wie es auch bei einer Übermittlung dieser Informationen an die Geheimschutzstelle des Deutschen Bundestages nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In der Abwägung zwischen dem parlamentarischen Informationsrecht der Abgeordneten einerseits und den im Staatswohl begründeten Geheimhaltungsinteressen andererseits muss das parlamentarische Informationsrecht daher ausnahmsweise zurückstehen. Dabei ist der Umstand, dass die Beantwortung verweigert wird, weder als Bestätigung noch als Verneinung des jeweiligen angefragten Sachverhalts zu werten.

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?

Die Bundesregierung berichtet den zuständigen Gremien des Deutschen Bundestages fortdauernd und anlassbezogen zu entsprechenden Themen.

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?

Das Bundesamt für Sicherheit in der Informationstechnik wird von den Behörden nach Maßgabe der geltenden Rechtslage sowie gegebenenfalls zusätzlich auf Basis eigener Bedarfe eingebunden. Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die Fragen 3 bis 3b werden gemeinsam beantwortet.

Das Bundeskriminalamt prüft die Instrumente der informationstechnischen Überwachung, die es für seine Ermittlungen benutzt, vor deren Einsatzfreigabe. Die Prüfung umfasst die Einhaltung der rechtlichen Rahmenbedingungen und die Konformität unter anderem gemäß der „Standardisierenden Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung“. Darüber hinaus wird auf die Antworten zu den Fragen 1 und 2 verwiesen.

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?

Die betroffenen Behörden binden den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bei der Beschaffung, Abnahme und dem Einsatz von Produkten der informationstechnischen Überwachung im Rahmen der geltenden Rechtslage ein.

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

Es wird auf die Antwort zu Frage 3 sowie auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Es wird auf die Antwort zu Frage 3 sowie auf die Vorbemerkung der Bundesregierung verwiesen. Hinsichtlich der Überprüfung und Abnahme von Ermittlungsinstrumenten der informationstechnischen Überwachung befinden sich die betroffenen Behörden in einem kontinuierlichen Austausch.

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

Es wird auf die Antworten zu den Fragen 1, 2, 4 und 6 sowie auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Es wird auf die Antwort zu Frage 3 verwiesen.

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

Bei der Beantragung richterlicher Anordnungen zur Durchführung von Maßnahmen der informationstechnischen Überwachung werden dem anordnenden Gericht die notwendigen verfahrensbezogenen Informationen gemäß den geltenden gesetzlichen Bestimmungen zur Verfügung gestellt.

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?

Die Fragen 10 und 11 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

In Bezug auf im Rahmen von Ermittlungsverfahren im Bereich der Strafverfolgung durchgeführte Maßnahmen der informationstechnischen Überwachung durch Polizei- beziehungsweise Strafverfolgungsbehörden des Bundes und der Länder wird auf die durch das Bundesamt für Justiz regelmäßig veröffentlichten justiziellen Statistiken über Maßnahmen der Telekommunikationsüberwachung und der informationstechnischen Überwachung im Rahmen der Strafverfolgung verwiesen. Darüber hinaus wird im Hinblick auf Maßnahmen des Bundeskriminalamtes gemäß Abschnitt 5 und §§ 34 und 64 des Bundeskriminalamtgesetzes (BKAG) auch auf den aktuellen Bericht des Bundeskriminalamtes gemäß § 88 BKAG verwiesen. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Der Bundesregierung liegen zu dieser Fragestellung keine über die in öffentlichen Facharbeiten und Berichterstattungen zum diesbezüglichen Stand der Technik beschriebenen Sachverhalte hinausgehenden Informationen vor.

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?

Die Bundesregierung geht grundsätzlich davon aus, dass sich Vertragspartner von Bundesbehörden an die in geschlossenen Verträgen festgehaltenen Rahmenbedingungen halten.

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?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die Fragen 16 und 17 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Befassung mit rechtlichen Fragen des verfassungskonformen Einsatzes von Produkten und Leistungen im Bereich der informationstechnischen Überwachung (ITÜ) obliegt den Behörden, die die ITÜ-Maßnahmen im Rahmen ihrer gesetzlichen Befugnisse durchführen. Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) selbst verfügt über keine gesetzlichen Befugnisse zur Durchführung von ITÜ-Maßnahmen. Im Übrigen wird auf die Antwort zu Frage 3 verwiesen.

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?

Die ZITiS steht in einem kontinuierlichen Austausch mit ihren Bedarfsträgern bezüglich technischer Fragestellungen zu möglichen Ermittlungsinstrumenten der informationstechnischen Überwachung. Nähere Ausführungen zu konkreten Einsätzen oder Einsatzaspekten können unter Verweis auf die Vormerkung der Bundesregierung nicht gemacht werden.

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)?

Zur Erhaltung und Verbesserung von Maßnahmen der informationstechnischen Überwachung führen die Sicherheitsbehörden und ZITiS fortlaufende Erhebungen des aktuellen Produktportfolios bei verschiedenen Anbietern, Herstellern und Behörden durch. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die Ausfuhr von Software zur informationstechnischen Überwachung unterfällt nach Kenntnis der Bundesregierung grundsätzlich der Exportkontrolle durch das israelische Verteidigungsministerium. Weiter liegen der Bundesregierung keine über die Medienberichterstattung, unter anderem hinsichtlich einer erfolgten Verschärfung der Exportbeschränkung durch die israelische Regierung, hinausgehenden Erkenntnisse vor.

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?

Der Aufbau und die Entwicklung des israelischen Cybersektors in seiner Gesamtheit basiert nach Kenntnis der Bundesregierung auf einer strategischen Entscheidung der Regierung aus dem Jahr 2011. Rechtliche Grundlage ist der Kabinettsbeschluss der Regierung Nr. 3611 vom 7. August 2011 („Advancing National Cyberspace Capabilities“, abrufbar unter www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing%20National%20Cyberspace%20Capabilities.pdf), die durch weitere Beschlüsse ergänzt wurde.

Im Rahmen der Cybersicherheitsstrategie 2021 der Bundesregierung wurde die Stärkung der digitalen Souveränität der deutschen Sicherheitsbehörden durch den Ausbau der ZITiS als strategisches Ziel vorgesehen. ZITiS soll in die Lage versetzt werden, Werkzeuge und Methoden zu entwickeln, zu bewerten und zentral zur Verfügung zu stellen, die den Sicherheitsbehörden ein selbstbestimmtes Handeln ermöglichen, eine krisenfeste Versorgungssicherheit gewährleisten und deren Cyberfähigkeiten signifikant stärken.

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?

Die Agentur für Innovation in der Cybersicherheit GmbH arbeitet momentan an Projekten in den Themenfeldern „Sichere neuronale Mensch-Maschine-Interaktion“, „Encrypted Computing“, „Existenzbedrohende Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien“ sowie „Ökosystem vertrauenswürdige IT-Formal verifiziertes Basis-IT-System“. Aussagen zur Zusammenarbeit der Agentur für Innovation in der Cybersicherheit GmbH mit privatwirtschaftlichen Partnern können aufgrund laufender Ausschreibungen und Vergabeverfahren zum jetzigen Zeitpunkt noch nicht getroffen werden. Seitens der ZITiS werden aktuell keine gemeinsamen Projekte mit der Agentur für Innovation in der Cyber-Sicherheit in diesen Themenbereichen durchgeführt.

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