Schriftliche Frage der Abgeordneten Martina Renner
vom 16. Juni 2022
(Monat Juni 2022, Arbeits-Nr. 6/176)

Frage

Welche Erkenntnisse hat die Bundesregierung über den Verbleib bzw. die Speicherung der anlässlich von Maßnahmen der informationstechnischen Überwachung (Quellen-TKÜ) durch deutsche Behörden unter Einsatz der Software „Pegasus“ der Firma NSO Group Technologies erhobenen und an der Firma NSO Group zugehörigen Cloud- bzw. sonstigen Speichern ausgeleiteten Daten und inwiefern ist nach Kenntnis der Bundesregierung eine Verarbeitung und Speicherung dieser Daten durch Dritte im Ausland über vertragliche Vereinbarungen und Zusagen hinaus technisch oder tatsächlich ausgeschlossen (https://www.washingtonpost.com/nationalsecurity/2022/06/14/l3harris-nso-sale-pegasus/; Drs. 20/321, Antwort zu Nr.14)?

Antwort

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 dieser Frage nicht erfolgen kann. Aus den im Rahmen einer Beantwortung der Frage erteilten Auskünften ließe sich ableiten, ob oder ob nicht die Software „Pegasus“ der Firma NSO Group Technologies durch Sicherheitsbehörden des Bundes eingesetzt wird. Einem öffentlichen Bekanntwerden dieser Informationen stehen überwiegende Belange des Staatswohls entgegen. Mit den aus diesen Auskünften ableitbaren Informationen über gegebenenfalls zur Verfügung oder nicht zur Verfügung stehende kriminaltaktische bzw. nachrichtendienstliche Vorgehensweisen und damit zu konkreten Maßnahmen oder Ermittlungs-/Analysefähigkeiten würde die Bundesregierung polizeiliche bzw. nachrichtendienstliche Vorgehensweisen zur Gefahrenabwehr oder zur Verhinderung und Aufklärung von Straftaten offenlegen oder Rückschlüsse darauf ermöglichen und damit die Arbeitsfähigkeit und Aufgabenerfüllung der Sicherheitsbehörden bzw. Nachrichtendienste gefährden, weil Täter oder potentielle Zielpersonen ihr Verhalten anpassen und künftige Maßnahmen dadurch erschweren oder gar vereiteln könnten. Eine Preisgabe solcher sensiblen Informationen würde sich auf die staatliche Aufgabenwahrnehmung im Gefahrenabwehrbereich wie auch auf die Durchsetzung des Strafverfolgungsanspruchs und die nachrichtendienstliche Informationsbeschaffung außerordentlich nachteilig auswirken.

Einzelne Kooperationspartner arbeiten mit den Nachrichtendiensten des Bundes nur unter der Voraussetzung zusammen, dass die konkrete Kooperation mit ihnen - auch nicht mittelbar - preisgegeben, sondern absolut vertraulich behandelt wird. Dies bedeutet, dass die geheimhaltungsbedürftigen Informationen zu und aus der Kooperation nicht außerhalb der betroffenen Stellen weitergegeben werden dürfen. Eine Offenlegung der Kooperationspartner würde das Ansehen von deutschen Nachrichtendiensten und das Vertrauen in diese daher weltweit erheblich schädigen. Dementsprechend bestünde die ernstzunehmende Gefahr eines weitreichenden Wegfalls von Kooperationsmöglichkeiten nicht nur bei zivilen Firmen. Würde die Bundesregierung die Informationen freigeben, so wäre zudem zu befürchten, dass Kooperationspartner ihrerseits die Vertraulichkeit nicht oder nur noch eingeschränkt wahren würden. In der Konsequenz könnte es künftig zu einem Rückgang oder zum Wegfall zukünftiger Vertragspartner und in der Folge zu einem Wegfall der Erkenntnisgewinnung der deutschen Nachrichtendienste kommen. Dies alles würde dem deutschen Staatswohl zuwiderlaufen. Dies hätte signifikante Informationslücken und negative Folgewirkungen für die Abbildung der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland zur Folge.

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 Aufklärung bzw. Ermittlungsunterstützung für die Aufgabenerfüllung der Sicherheitsbehörden bzw. Nachrichtendienste des Bundes nicht in Betracht. Auch ein geringfügiges Risiko des Bekanntwerdens derart sensibler Informationen kann unter keinen Umständen hingenommen werden. Die angefragten Inhalte beschreiben die technischen Fähigkeiten der betroffenen Sicherheitsbehörden bzw. Nachrichtendienste des Bundes in einem durch den Bezug auf bestimmte Produkte derartigen Detaillierungsgrad, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Bei einem Bekanntwerden der schutzbedürftigen Informationen wäre der Einsatzerfolg der betroffenen Ermittlungs- bzw. Aufklärungsinstrumente stark gefährdet, da Abwehrstrategien dagegen entwickelt werden könnten. Dies würde einen erheblichen Nachteil für die wirksame Aufgabenerfüllung der betroffenen Sicherheitsbehörden bzw. Nachrichtendienste des Bundes bedeuten, und es wäre kein Ersatz durch andere Instrumente möglich.

Daraus folgt, dass die erbetenen Informationen derartig schutzbedürftige evidente Geheimhaltungsinteressen berühren, dass auch das geringfügige Risiko eines Bekanntwerdens, wie es auch bei einer Übermittlung dieser Informationen an die Geheimschutzstelle des Deutschen Bundestags nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In der Abwägung des parlamentarischen Informationsrechts der Abgeordneten einerseits und der im Staatswohl begründeten Geheimhaltungsinteressen der Bundesregierung andererseits muss das parlamentarische Informationsrecht daher ausnahmsweise zurückstehen. Dabei ist der Umstand, dass die Antwort verweigert wird, weder als Bestätigung noch als Verneinung o. g. Sachverhalts hinsichtlich einer Nutzungs- oder Nichtnutzungsmöglichkeit der in Bezug genommenen Software zu werten.