Deutscher Bundestag **Drucksache 20/9125**

20. Wahlperiode 07.11.2023

Kleine Anfrage

der Abgeordneten Martina Renner, Nicole Gohlke, Gökay Akbulut, Clara Bünger, Anke Domscheit-Berg, Dr. André Hahn, Susanne Hennig-Wellsow, Ina Latendorf, Cornelia Möhring, Petra Pau, Sören Pellmann, Dr. Petra Sitte, Kathrin Vogler und der Fraktion DIE LINKE.

Einsatz von Produkten der Unternehmensgruppe „Intellexa-Alliance“ zur informationstechnischen Überwachung durch deutsche Sicherheitsbehörden sowie Maßnahmen der Exportkontrolle bei Überwachungssoftware

Während im EU-Parlament mit dem Sonderausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (sogenannter PEGA-Ausschuss) eine Untersuchung zum Einsatz der Spähsoftware Pegasus der NSO Group Technologies in der EU stattfand und immer neue Details zur Ausspähung und zu fragwürdigen Einsätzen der Software bekannt wurden (vgl. u. a. https://netzpolitik.org/2022/pegasus-untersuchungsausschuss-die-regeln-an-sich-sind-schon-mangelhaft/; https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-projekt-103.html), wurde das EU-Mitglied Griechenland von einem sehr ähnlichen Abhörskandal durch den Einsatz von Überwachungssoftware erschüttert. So sollen laut Medienberichten mutmaßlich auf Anordnung des konservativen Regierungschefs u. a. Politikerinnen und Politiker der verschiedensten Parteien und Journalistinnen und Journalisten mittels der Spähsoftware „Predator“ überwacht und ausgespäht worden sein sollen (https://www.tagesschau.de/ausland/europa/griechenland-pegasus-abhoerskandal-101.html; https://www.spiegel.de/netzwelt/netzpolitik/predator-files-wie-intellexa-jahrelang-despoten-mit-spionageprogrammen-versorgte-a-0268f613-6b56-48e7-822f-0eccb85ae5c9). Weitere Fälle des Einsatzes der Spähsoftware „Predator“ betreffen beispielsweise ägyptische Oppositionspolitiker (https://www.spiegel.de/netzwelt/netzpolitik/predator-files-wie-intellexa-jahrelang-despoten-mit-spionageprogrammen-versorgte-a-0268f613-6b56-48e7-822f-0eccb85ae5c9; https://netzpolitik.org/2023/aegypten-oppositionspolitiker-mit-staatstrojaner-predator-ueberwacht/; https://balkaninsight.com/2022/01/06/wine-weapons-and-whatsapp-a-skopje-spyware-scandal/), vietnamesische Journalisten und u. a. die deutsche Botschafterin in Vietnam, Politiker und Institutionen der Europäischen Union (https://www.spiegel.de/netzwelt/netzpolitik/cyberspionage-und-digitale-ueberwachung-man-kann-sich-kaum-schuetzen-a-33ebeb75-ef20-4e77-ad12-da52b0b97a2f; https://www.spiegel.de/netzwelt/netzpolitik/predatorfiles-wie-vietnam-eine-deutsche-botschafterin-zu-hacken-versuchte-a-1d87a7d4-bb5c-4fa4-8824-c63d499be2f5). Die journalistische Recherche zum Einsatz von „Predator“ legte offen, dass die beteiligten Unternehmen offenbar auch versuchen, Exportbeschränkungen zu umgehen und es sich um ein verzweigtes Netz aus sich teils umbenennenden Unternehmen mit Dependancen und Tochterunternehmen in verschiedenen europäischen Ländern handelt (https://www.spiegel.de/netzwelt/netzpolitik/predator-files-wie-intellexa-jahrelang-despoten-mit-sp

ionageprogrammen-versorgte-a-0268f613-6b56-48e7-822f-0eccb85ae5c9; https://balkaninsight.com/2022/01/06/wine-weapons-and-whatsapp-a-skopje-spyware-scandal/). Eines der mutmaßlich beteiligten Unternehmen „Nexa Technoligies“ soll unter seinem früheren Namen „Amesys“ bereits 2006 Überwachungssoftware an den lybischen Herrscher Muammar al-Gaddafi verkauft haben und sieht sich deshalb Klagen und Ermittlungen gegenüber (https://www.spiegel.de/netzwelt/netzpolitik/predator-files-wie-intellexa-jahrelang-despoten-mit-spionageprogrammen-versorgte-a-0268f613-6b56-48e7-822f-0eccb85ae5c9; https://netzpolitik.org/2013/funf-libyerinnen-klagen-gegen-den-franzosischen-uberwachungslieferanten-amesys/). Auf der Homepage von „Nexa Technoligies“ heißt es nunmehr zur Begründung, dass künftig keine offensiven Cyberwaffen mehr angeboten würden: „Tatsächlich bieten die Verfahren zur ‚Exportkontrolle‘ von Cyber-Intelligence-Aktivitäten sowie der Rahmen für den Einsatz dieser Art von Instrumenten den Akteuren angesichts der anstehenden Probleme keinen ausreichend zuverlässigen Schutz. Mittelständische Unternehmen wie unseres, die nicht über die nötige geopolitische Expertise verfügen, um Rechts- und Reputationsrisiken vollständig zu verstehen, können daher trotz aller Vorsichtsmaßnahmen ungerechtfertigten Vorwürfen ausgesetzt sein“ (https://www.nexatech.fr/). Diese Rechtfertigung wirkt angesichts der früheren Geschäfte mit dem lybischen Diktator und den in den aktuellen Veröffentlichungen dargestellten Geschäftspraktiken, auch zur Umgehung von Exportbeschränkungen, nach Ansicht der Fragesteller kaum glaubhaft. Sollten Behörden des Bundes tatsächlich und weiterhin vertragliche Beziehungen mit den genannten Firmen pflegen und Produkte derselben erwerben und einsetzen wollen, müssten sie dabei auch berücksichtigen, dass einige dieser Firmen und ihre Produkte nach Einschätzung der US-amerikanischen Regierung eine Gefahr für die nationale Sicherheit und die außenpolitischen Interessen der USA und für die Verletzung amerikanischer Sicherheitsinteressen darstellen und deshalb Handelsbeschränkungen unterliegen (https://www.washingtonpost.com/national-security/2023/07/18/entity-list-spyware-intellexa-cytrox/). Offen ist, ob diese Handelsbeschränkungen auch die deutschen Risikokapitalgeber (https://www.spiegel.de/netzwelt/netzpolitik/predator-files-wie-intellexa-jahrelang-despoten-mit-spionageprogrammen-versorgte-a-0268f613-6b56-48e7-822f-0eccb85ae5c9; https://www.presseportal.de/pm/112110/4221936) betreffen, die die Geschäfte dieser Unternehmen maßgeblich finanzierten.

Wir fragen die Bundesregierung:

1. Haben Vertreter oder Beauftragte der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. von Tochterunternehmen der vorgenannten Unternehmen Behörden oder Stellen des Bundes bzw. den Vertretern der Behörden die von ihnen entwickelten und vertriebenen Softwareprodukte zur Infiltration und Überwachung informationstechnischer Systeme und Netzwerke, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung vorgestellt bzw. angeboten, und wenn ja, wann welchen Behörden oder Stellen (bitte nach Jahr, Behörde, Unternehmen und Produkt auflisten)?
2. Welche Produkte der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen wurden bzw. werden von Einrichtungen oder Stellen des Bundes auf ihre Einsatzmöglichkeit unter Berücksichtigung der jeweils geltenden Rechtslage oder im Hinblick auf künftig mögliche Einsatzmög-

lichkeiten geprüft (bitte Name des Produkts, prüfende Behörde und mögliche Einsatzzwecke sowie seit bzw. von wann bis wann die Prüfung erfolgte bzw. erfolgt, angeben)?

3. Waren Produkte und Leistungen zur informationstechnischen Überwachung oder zur Massendatenanalyse und Massendatenverarbeitung im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen Gegenstand der Marktsichtung durch die Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) oder andere Bedarfsträger im Geschäftsbereich der Bundesregierung?

4. Wann, und mit welchem Ergebnis haben sich ZITiS oder andere Bedarfsträger im Geschäftsbereich der Bundesregierung mit Produkten und Leistungen im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung beschäftigt?

5. Wer wurde von ZITiS oder von anderen Bedarfsträgern im Geschäftsbereich der Bundesregierung wann über das Ergebnis dieser Marktsichtung unterrichtet, und wie hat die zuständige Fach- und Rechtsaufsicht sich zu diesem Prüfergebnis verhalten?

6. Inwieweit wurde ZITis von der Prüfung, dem Einsatz, einschließlich von Test- oder Erprobungseinsätzen von Produkten und Leistungen im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung durch andere Behörden und Stellen des Bundes wann in Kenntnis gesetzt oder hat Kenntnis von technischen Fragen und Problemstellungen im Rahmen von Prüfung bzw. Einsatz (etwa zum Aufbau von Know-how für zukünftige Beschaffungen in diesem Bereich) durch andere Behörden und Stellen des Bundes erhalten?

7. Hat die Bundesregierung alle ggf. infrage kommenden Gremien des Deutschen Bundestages über Prüfung, Ankauf und Einsatz, einschließlich von Test- oder Erprobungseinsätzen von Produkten und Leistungen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen durch Behörden im Zuständigkeitsbereich dieser Gremien unterrichtet, und wenn nein, warum ist eine solche Unterrichtung bislang unterblieben?

8. Wurde eine technische Prüfung der Produkte und Leistungen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Hol-

dings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen durch das Bundesamt für Sicherheit in der Informationstechnik durchgeführt, wenn ja, wann, und mit welchem Ergebnis, und wenn nein, warum nicht?

9. Nach welchen Kriterien, Schemata, fachlichen Vorgaben oder Fragestellungen wurde ggf. eine Überprüfung der Produkte und Leistungen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen durch die einsetzenden Behörden bzw. Bedarfsträger selbst vorgenommen?

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

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

12. Waren die geschäftsführenden Bundesministerien anlässlich bzw. im Nachgang über den Einsatz und über die Ergebnisse von Überprüfungen der Produkte und Leistungen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen informiert, und wenn ja, wer wurde jeweils wann und worüber unterrichtet?

13. Hat sich nach Kenntnis der Bundesregierung infolge von Überprüfungen bzw. Auswertungen des Einsatzes ergeben, dass die Behörden des Bundes zur Verfügung gestellte Programmversionen von Produkten und Leistungen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen weiterer Einschränkungen bedürfen, und wenn ja, seit wann ist das bekannt geworden, und wann wurde dies entsprechend umgesetzt?

14. Welche Informationen über Produkte und Leistungen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen wurden den zuständigen Kontrollgremien bzw. Gerichten zu Verfügung gestellt, die den Einsatz im Rahmen von Gefahrenabwehrvorgängen oder Strafermittlungen bzw. als nachrichtendienstliches Mittel genehmigt bzw. angeordnet haben?

15. In wie vielen Fällen mit wie vielen Betroffenen wurden Produkte und Leistungen zur informationstechnischen Überwachung, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung im Angebot der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen bislang nach Kenntnis der Bundesregierung 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 (Fernmeldeaufklärung, nachrichtendienstliches Mittel, Gefahrenabwehr, Strafverfolgung)?

16. In wie vielen Fällen der in Frage 15 erfragten Fälle handelte es sich um das Produkt „Cerebro“ (vormals „Eagle“) des Unternehmens „Advanced Middle East Systems“ (Ames)?

17. In wie vielen Fällen der in Frage 15 erfragten Fälle handelte es sich um das Produkt „Predator“ der Unternehmen „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. den Tochterunternehmen der vorgenannten Unternehmen?

18. 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?

19. Welchen Schweregrad (base score) nach dem Common Vulnerability Scoring System (CVSS) haben nach Kenntnis der Bundesregierung die beim Einsatz der Produkte der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen genutzten Vektoren zur Ausleitung von Daten aus dem jeweiligen Zielsystem?

20. Welche Kosten sind jeweils durch die Beschaffung, den Betrieb und die Wartung von Produkten der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen für Behörden des Bundes bislang entstanden (bitte nach Behörde und Jahr aufschlüsseln)?

21. Wurden deutsche Behörden seitens anderer EU-Mitgliedstaaten im Rahmen der Rechtshilfe um Unterstützung bzw. Durchführung von Ermittlungsmaßnahmen hinsichtlich der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“, „Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen ersucht, und wenn ja, wann durch welche europäischen Behörden?

22. In wie vielen Fällen wurden nach Kenntnis der Bundesregierung informationstechnische Systeme oder Telekommunikationssysteme deutscher Behörden und Stellen bzw. deutscher Bürgerinnen und Bürger mit Produkten der Unternehmen „Intellexa S.A.“, „Intellexa Limited“, „Nexa Technoligies“, „Advanced Middle East Systems“ (Ames), „Aliada Group Inc.“,

„Cytrox Holdings CRT“, „Cytrox AD“, der Unternehmensgruppe „Intellexa-Alliance“ bzw. der Tochterunternehmen der vorgenannten Unternehmen infiltriert und Daten bzw. Kommunikationsvorgänge mitgelesen, verändert, überwacht, ausgeleitet oder dergleichen versucht (bitte nach Behörden und Personen, Art der Detektion und erfolgtem Datenabfluss auflisten)?

23. Welche Schlussfolgerungen wird die Bundesregierung im Falle des Nachweises einer Detektion wie in Frage 22 für etwaig bestehenden Kontakte oder Verträge mit den Personen, Unternehmern oder Institutionen, die für die Herstellung, den Vertrieb und die Finanzierung der verwendeten Softwareprodukte ziehen?

24. Welche Schlussfolgerungen ergeben sich aus Sicht der Bundesregierung und ihrer nachgeordneten Behörden aus der Entscheidung der US-amerikanischen Regierung über Sanktionen und Handelsbeschränkungen gegen die Unternehmen „Intellexa S.A.“, „Cytrox Holdings Crt“, „Cytrox AD“ und „Intellexa Limited“?

25. Welche Schlussfolgerungen ergeben sich aus Sicht der Bundesregierung und ihrer nachgeordneten Behörden aus den im Rahmen der Veröffentlichungen bekannt gewordenen Vorgehensweisen zur Umgehung von Normen und Regeln der Exportkontrolle (vgl. Vorbemerkung der Fragesteller), und werden nach Kenntnis der Bundesregierung in diesem Zusammenhang Vorprüfungen, Untersuchungen oder Ermittlungen geführt, und wenn ja, welche durch welche Behörde?

26. Erachtet die Bundesregierung die Regelungen zur Exportkontrolle von Dual-Use-Gütern wie Softwareprodukte zur Infiltration und Überwachung informationstechnischer Systeme und Netzwerke, zum Targeted Advertising sowie zur Massendatenanalyse und Massendatenverarbeitung angesichts der durch die in der Vorbemerkung der Fragesteller aufgeführten Veröffentlichungen bekannt gewordenen Vorgehensweisen zur Umgehung von Normen und Regeln der Exportkontrolle als ausreichend, oder inwieweit sind aus Sicht der Bundesregierung Korrekturen beispielsweise zur Haftung von Unternehmern oder Risikokapitalgebern zu prüfen und einzuführen?

27. Mit welcher Begründung hat sich die Bundesregierung nicht der sog. Anti-Spyware Declaration von elf Ländern (darunter die Regierungen von Australien, Kanada, Costa Rica, Dänemark, Frankreich, Neuseeland, Norwegen, Schweden, der Schweiz, dem Vereinigten Königreich und den USA) zur Bekämpfung der Verbreitung und des Missbrauchs kommerzieller Spionagesoftware angeschlossen, und inwiefern erwächst nach Auffassung der Bundesregierung konkreter (gesetzgeberischer) Handlungsbedarf aus den Abschlussempfehlungen des Untersuchungsausschusses des Europäischen Parlaments zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware, dem Beschluss der parlamentarischen Versammlung des Europarates (Resolution 2513 (2023)) sowie dem Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP (z. B. Verschärfung der Exportregulierung, Stärkung gerichtliche sowie parlamentarische Kontrolle, usw.; bitte je geplanter Maßnahme auch jeweiligen Stand anführen)?

Berlin, den 27. Oktober 2023

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.bundesanzeiger-verlag.de
ISSN 0722-8333