Deutscher Bundestag **Drucksache 20/9455**

20. Wahlperiode 22.11.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Martina Renner, Nicole Gohlke, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 20/9125 –

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

Vorbemerkung der Fragesteller

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

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 17. November 2023 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

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-spionageprogrammen-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.

Vorbemerkung der Bundesregierung:

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich öffentlich, transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit erfragte Informationen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann, und gegebenenfalls alternative Formen der Informationsvermittlung zu suchen, die das Informationsinteresse des Parlaments unter Wahrung der berechtigen Geheimhaltungsinteressen der Regierung befriedigen (BVerfGE 124, S. 161, 193). Evident geheimhaltungsbedürftige Informationen muss die Bundesregierung nach der Rechtsprechung des Bundesverfassungsgerichts nicht offenlegen (BVerfGE 124, 161, 193 f.).

Soweit die Fragen nicht explizit an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) gerichtet sind, geht die Bunderegierung im Kontext der Fragestellung davon aus, dass sich die Fragen auf die Strafverfolgungs-, Ermittlungs- und Gefahrenabwehrbehörden des Bundes sowie der Nachrichtendienste des Bundes beziehen. Dementsprechend werden ausschließlich diese in die Beantwortung einbezogen.

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 1 bis 5 sowie 7 bis 25 bezüglich der Strafverfolgungs-, Ermittlungs- und Gefahrenabwehrbehörden des Bundes sowie der Nachrichtendienste des Bundes aufgrund entgegenstehender überwiegender Belange des Staatswohls nicht bzw. teilweise nicht erfolgen kann, auch nicht in eingestufter Form.

Die insoweit erbetenen Informationen zielen auf die kriminaltaktischen oder nachrichtendienstlichen Ermittlungs- bzw. Informationsgewinnungsinstrumente der betroffenen Sicherheitsbehörden ab. Mit der Beantwortung würden mittelbar bestimmte Arbeitsmethoden und Vorgehensweisen im Bereich der technischen Aufklärung offengelegt oder Rückschlüsse darauf ermöglicht. Hierdurch würden die Arbeitsfähigkeit und Aufgabenerfüllung und somit die Erfüllung des gesetzlichen Auftrags der betroffenen Sicherheits- und Strafverfolgungsbehörden sowie Nachrichtendienste erheblich gefährdet.

Schon die Angabe, mit welchen Herstellern technischer Produkte im Bereich der informationstechnischen Überwachung die betroffenen Sicherheitsbehörden in Kontakt stehen und damit mittelbar die Angabe, welche technischen Produkte die Sicherheitsbehörden in diesem sensiblen Bereich derzeit oder zukünftig einsetzen könnten, kann zu einer gezielten Änderung des Kommunikationsverhaltens der betreffenden zu beobachtenden Personen führen, wodurch eine weitere Aufklärung der von diesen Personen verfolgten Bestrebungen und Planungen unmöglich werden würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung der Sicherheitsbehörden des Bundes nicht in Betracht. Das Risiko, dass derart sensible Informationen bekannt werden, kann unter keinen Umständen hingenommen werden. Die angefragten Informationen beschreiben die technischen Fähigkeiten der betroffenen Sicherheitsbehörden bzw. Nachrichtendiensten des Bundes aufgrund ihres Bezuges auf bestimmte Produkte bzw. 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 erbetenen Informationen derartig schutzbedürftig sind, dass auch eine Hinterlegung in der Geheimschutzstelle des Deutschen Bundestages aus Staatswohlgründen nicht in Frage kommt. In der Abwägung des parlamentarischen Informationsrechts der Abgeordneten einerseits und der staatswohlbegründeten 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. 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 Einsatzmöglichkeiten geprüft (bitte Name des Produkts, prüfende Behörde und mögliche Einsatzzwecke sowie seit bzw. von wann bis wann die Prüfung erfolgte bzw. erfolgt, angeben)?

Die Fragen 1 und 2 werden gemeinsam beantwortet.

Die gewünschten Informationen können nicht übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die Fragen 3 bis 5 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Zur Wahrnehmung ihrer Aufgaben hinsichtlich der Weiterentwicklung von Cyberfähigkeiten im Bereich der Informationstechnischen Überwachung steht die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) mit Vertretern des Unternehmens „Intellexa“ bzw. deren Tochterunternehmen „CYTROX“ in Kontakt, um im Rahmen einer Marktsichtung Informationen

über das Portfolio des Unternehmens zu erhalten. Dies beinhaltet ebenso eine Beschäftigung mit den von dem Unternehmen angebotenen Produkten und Leistungen.

Nähere Ausführungen zu konkreten Ergebnissen können unter Verweis auf die Vorbemerkung der Bundesregierung nicht gemacht werden.

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?

Zum Erhalt und zur Verbesserung von Maßnahmen der informationstechnischen Überwachung sowie der Massendatenanalyse steht die ZITiS fortlaufend mit den Sicherheitsbehörden im Austausch. Nähere Ausführungen zu konkreten Einsätzen oder Einsatzaspekten können unter Verweis auf die Vorbemerkung der Bundesregierung nicht gemacht werden.

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?

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

Darüber hinaus können die gewünschten Informationen nicht übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

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 Holdings 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?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird von den Behörden nach Maßgabe der geltenden Rechtslage sowie gegebenenfalls zusätzlich auf Basis eigener Bedarfe eingebunden.

Darüber hinaus können die gewünschten Informationen nicht übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die Fragen 9 bis 11 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die gewünschten Informationen können nicht übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die hier in Rede stehenden Behörden berichten den die Fachaufsicht führenden Bundesministerien regelmäßig über relevante Sachverhalte. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die gewünschten Informationen können nicht übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

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

Darüber hinaus wird auf die Antwort zu Frage 7 verwiesen.

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?

Die Fragen 15 bis 18 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die gewünschten Informationen können nicht übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die Fragen 19 bis 23 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die gewünschten Informationen können nicht übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die Fragen 24 bis 26 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Mit der neuen Dual-Use-Verordnung, auf die sich der Rat der Europäischen Union am 9. November 2020 unter deutschem Vorsitz mit dem Europäischen Parlament geeinigt hat, ist es gelungen neue, striktere Kontrollvorschriften für Ausfuhren bestimmter Abhör- und Überwachungstechnik einzuführen. Damit konnte auf die deutsche Initiative aufgesetzt werden, Ausfuhren bestimmter Überwachungstechnologien im Wassenaar Abkommen international zu kontrollieren. Darüber hinaus hatte Deutschland bereits Mitte 2015 zusätzliche nationale Kontrollen für den Export von Monitoringsystemen für Telefonie und entsprechender Vorratsdatenspeicherung eingeführt. Die Bundesregierung setzt sich dafür ein, dass verbleibende Kontrolllücken bei Überwachungstechnologie auch auf internationaler Ebene geschlossen werden. Auf Initiative Deutschlands wurden im Jahr 2019 im sogenannten Wassenaar-Arrangement neue Kontrollen für Ausfuhren von Software zur Telefonüberwachung vereinbart. Damit konnten die seit dem Jahr 2015 in Deutschland bereits auf nationaler Ebene bestehenden Kontrollen für die Monitoringsysteme erfolgreich auch auf internationaler Ebene verankert werden.

Die Bundesregierung verfolgt eine restriktive Exportkontrollpolitik. Jeder Einzelfall wird auf die beabsichtigte konkrete Nutzung des Dual-Use-Guts beim Endverwender im Empfängerland geprüft. Dabei wendet die Bundesregierung die einschlägigen Rechtsvorschriften strikt an. Auch die Verhinderung von Umgehungslieferungen sind der Bundesregierung ein wichtiges Anliegen.

Darüber hinaus können hinsichtlich der Fragen 24 und 25 die gewünschten Informationen nicht übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

Im Übrigen äußert sich die Bundesregierung nicht zu laufenden Ermittlungsverfahren.

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)?

Die Bundesregierung bewertet die Zielrichtung der gemeinsamen Erklärung grundsätzlich positiv. Zentral sind der umfassende Schutz von Menschenrechten und sonstigen fundamentalen Rechten, sowie das Zusammenspiel mit und der Mehrwert gegenüber bestehenden Verpflichtungen. Dies gilt gleichermaßen für die analoge wie für die digitale Welt. Hierfür setzt sich die Bundesregierung, auch gemeinsam mit ihren Partnern, aktiv ein. Deutschland unterstützt die in der Erklärung genannten „Guiding Principles on Government Use of Surveillance Technologies“.

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