BREMISCHE BÜRGERSCHAFT **Drucksache 20/1536**
Landtag
20. Wahlperiode **13. Juli 2022**

Große Anfrage der Fraktion Bündnis 90/Die Grünen

Quellen-Telekommunikationsüberwachung und Online-Durchsuchung – Mogelpackung auf Kosten der IT-Sicherheit?

Computer und Smartphones enthalten heutzutage oft eine unermessliche Fülle an Informationen: alltägliche bis intimste E-Mails, SMS und Messenger-Nachrichten, Terminkalender, Kontakte, Gesundheitsdaten von angeschlossenen Fitness-Trackern, Kontoumsätze, Geodaten, Tagebücher und Social-Media-Accounts. Mit Speicherkapazitäten im Giga- bis Terabyte-Bereich enthalten sie ein weitgehendes digitales Abbild unseres Lebens. Das Bremische Polizeigesetz und die Strafprozessordnung enthalten Rechtsgrundlagen, um Computer und Smartphones bei den Betroffenen zu beschlagnahmen, wenn dies zur Gefahrenabwehr oder zur Strafverfolgung erforderlich ist. Diese Rechtsgrundlagen können auch heute bereits dazu genutzt werden, um Daten sicherzustellen, die auf einem Online-Speicher (Cloud) abgelegt sind. Dazu zählen nicht nur E-Mails, Dokumente und Fotos, sondern auch Nachrichten von cloud-basierten Messengern wie Telegram oder Facebook bis hin zu kompletten Geräte-Backups, mit denen die Sicherheitsbehörden auch auf die sonst nur lokal auf dem Gerät gespeicherten Inhalte Zugriff erhalten können. Insgesamt ergeben sich auf diese Weise für die Sicherheitsbehörden Zugriffsmöglichkeiten auf Informationen in einem Umfang, der in früheren Jahrzehnten undenkbar erschien. Die Herausforderung für Ermittler*innen besteht heute oft weniger darin, zusätzliche Informationen zu erlangen, sondern in der nutzbaren Auswertung der riesigen Datenmengen.

Vor diesem Hintergrund erscheinen Aussagen, die Sicherheitsbehörden könnten aufgrund der zunehmenden Verbreitung verschlüsselter Internetkommunikation kaum noch auf diese Inhalte dieser Kommunikation zugreifen und daher schlimmste Verbrechen nicht mehr verhindern oder aufklären, wenig belastbar. Dennoch gibt es auf Bundesebene und in mehreren Bundesländern mit der Online-Durchsuchung und der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) weitergehende Befugnisse. Diese sollen den Sicherheitsbehörden ermöglichen, auf Computer und Smartphones zuzugreifen, ohne dass die Zielperson dies bemerkt, wie es bei einer Sicherstellung unweigerlich der Fall wäre, und ohne dass der Zugriff über Cloud-Anbieter erfolgen muss, die oft im Ausland sitzen und nicht immer für deutsche Behörden erreichbar sind. Beide Instrumente, Quellen-TKÜ und Online-Durchsuchung stehen dem Bundeskriminalamt bereits seit 2008 und den bremischen Strafverfolgungsbehörden seit einer Änderung der Strafprozessordnung im Jahr 2017 zur Verfügung.

Abgesehen von der Nutzung regulärer Funktionen von Messenger-Apps, wie beispielsweise die Gerätekopplung unter Zuhilfenahme des Smartphones der Zielperson, kann der Zugriff auf die Endgeräte bei Online-Durchsuchung

und Quellen-TKÜ in der Regel nur durch Hacking erlangt werden, insbesondere per Trojaner. Dabei werden oft Sicherheitslücken in Soft- und Hardware genutzt, die den Herstellern noch unbekannt sind. Staatstrojaner sind für Sicherheitsbehörden nur dann sinnvoll nutzbar, wenn auf möglichst vielen unterschiedlichen Gerätetypen Sicherheitslücken vorhanden sind, die beim staatlichen Hacking ausgenutzt werden können. Das schafft Anreize für die anwendenden Stellen, ein „Arsenal“ von Sicherheitslücken aufzubauen und diese den Herstellern zu verheimlichen, damit sie nicht geschlossen werden. Jede einzelne Lücke in einer solchen elektronischen Waffenkammer kann allerdings nicht nur von Behörden für Hacks von Handys und Computern ausgenutzt werden, sondern auch von Kriminellen. Das gefährdet die Cybersicherheit in Deutschland und auf der ganzen Welt. Spürbar wurde dies einer breiteren Öffentlichkeit etwa im Jahr 2017, als die Erpresser-Software WannaCry weltweit hohe Schäden verursachte und unter anderem das britische Krankenhaussystem lahmlegte. WannaCry beruhte auf Sicherheitslücken in Microsoft Windows, die der US-Auslandsgeheimdienst NSA mindestens fünf Jahre lang genutzt hatte, ohne Microsoft zu informieren. Auch der Anfang Juli 2021 erfolgte Cyber-Angriff mit Verschlüsselungstrojanern auf zahlreiche IT-Dienstleister, deren Kunden und weitere Unternehmen in Deutschland und weltweit beruhte auf einer Sicherheitslücke in einer verbreiteten Software. Das Bundesverfassungsgericht hat vor diesem Hintergrund jüngst die grundrechtliche Schutzpflicht der Sicherheitsbehörden betont, bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke zu ermitteln und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ zu bestimmen, beides zueinander ins Verhältnis zu setzen und die Sicherheitslücke an den Hersteller zu melden, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt.

Die Verwendung von Staatstrojanern gefährdet nicht nur die IT-Sicherheit, sondern ist teilweise auch mit menschenrechtsverletzenden Geschäftspraktiken verbunden. Bundesregierung und deutsche Sicherheitsbehörden arbeiten seit Jahren mit Unternehmen der Überwachungsindustrie zusammen, die auf die Strategie setzen, zunächst Sicherheitslücken zu finden oder auf dem Schwarzmarkt von Kriminellen abzukaufen, dann mit Hilfe von Trojaner-Software unbemerkt in die IT-Systeme einzudringen und schließlich Daten an Sicherheitsbehörden aus aller Welt auszuleiten. Dabei ist es teilweise Geschäftspraxis dieser Unternehmen, ihre nicht zuletzt mit deutschen Steuermitteln finanzierten Produkte weltweit auch an Regierungen zu verkaufen, die damit Menschenrechtler*innen, Journalist*innen oder Oppositionelle ausspionieren. Dies zeigt unter anderem der Fall der Spionagesoftware FinSpy des britisch-deutschen Unternehmens FinFisher, das auch das Bundeskriminalamt mit Staatstrojaner-Software beliefert. Im Juli 2019 erstatteten mehrere Nichtregierungsorganisationen Strafanzeige wegen Verstoßes gegen § 18 des Außenwirtschaftsgesetzes gegen den Geschäftsführer von FinFisher. Dabei wurden umfangreiche Anhaltspunkte dafür vorgelegt, dass FinFisher die Spionagesoftware FinSpy ohne Genehmigung der Bundesregierung an die türkische Regierung verkauft und so zur Überwachung von Oppositionellen und Journalist*innen in der Türkei beigetragen haben soll. Nachdem sich der Tatverdacht offensichtlich erhärten ließ, durchsuchte die Staatsanwaltschaft München im Zuge der Ermittlungen gegen FinFisher vom 6. bis 8. Oktober 2020 15 Wohn- und Geschäftsräume im In- und Ausland. Ende 2021 erließ das Amtsgericht München einen Vermögensarrest, um die von der FinFisher-Gruppe mit rechtswidrigen Praktiken erlangten Einnah-

men für eine mögliche Einziehung zu sichern. Daraufhin meldeten drei Unternehmen der FinFisher-Gruppe Insolvenz an und stellten ihren Geschäftsbetrieb ein.

Verschiedene journalistische Recherchen haben zudem derart zahlreiche und schwerwiegende Ausspähungsskandale im Zusammenhang mit dem auch von deutschen Behörden eingesetzten Staatstrojaner Pegasus des israelischen Herstellers NSO Group ans Licht gebracht, dass das Europäische Parlament einen Untersuchungsausschuss „zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware“ eingesetzt hat. Der Europäische Datenschutzbeauftragte hat ein umfassendes Verbot der Entwicklung und des Einsatzes von Ausspähsoftware wie Pegasus in der gesamten Europäischen Union gefordert. Die Technologie stelle nicht nur eine Gefahr für Menschen und ihre Geräte dar, sondern auch für Demokratie und Rechtsstaatlichkeit.

Die rechtsstaatliche Kontrolle des Einsatzes staatlicher Spionagesoftware gestaltet sich in der Praxis tatsächlich schwierig. Bereits 2011 brachte eine Analyse des Chaos Computer Clubs ans Licht, dass ein von deutschen Strafverfolgungsbehörden damals zur Quellen-TKÜ verwendeter Staatstrojaner fast sämtliche verfassungsrechtlichen Vorgaben aufs Gröbste missachtete, ohne dass dies Staatsanwaltschaften oder Gerichten zuvor aufgefallen wäre. Der Einsatz von Staatstrojanern muss daher mit entsprechenden technischen Kompetenzen bei den beteiligten Stellen einhergehen. Zudem darf die parlamentarische Kontrolle nicht derart behindert werden, wie es gegenüber dem Deutschen Bundestag geschieht. Das Bundesinnenministerium begründete im Innenausschuss des Bundestags die weitgehende Verweigerung von Antworten auf diverse Kleine Anfragen so: „Die Unternehmen wollen nicht, dass es offenbar wird, dass sie mit der Bundesregierung oder mit Sicherheitsbehörden des Bundes kooperieren. Wenn dies der Fall ist, dann beenden sie ihre Geschäftsbeziehungen mit uns.“

Ungeachtet dessen wurde der Einsatz von Quellen-TKÜ mittlerweile auch auf Nachrichtendienste ausgeweitet. Seit dem 9. Juli 2021 enthält das Artikel-10-Gesetz die Befugnis zur Quellen-TKÜ. Da das Artikel-10-Gesetz nicht nur für das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst und Militärischen Abschirmdienst gilt, sondern auch für die Verfassungsschutzbehörden der Länder, darf jetzt auch das bremische Landesamt für Verfassungsschutz Staatstrojaner einsetzen. Anders als die bisherigen Regelungen zur Quellen-TKÜ in der Strafprozessordnung und im BKA-Gesetz werden die Internet-Provider im Artikel-10-Gesetz sogar verpflichtet, Internetverkehr an die Nachrichtendienste umzuleiten, um das Einschleusen und Installieren von Staatstrojanern zu erleichtern. Insbesondere gegen diese Neuerung wendet sich eine breite Initiative aus zivilgesellschaftlichen Organisationen und Unternehmen, die vom Chaos Computer Club (CCC) über Google und Facebook bis hin zum Bundesverband IT-Mittelstand (MITMi), dem Verband der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM) und dem Verband der Internetwirtschaft (eco) reicht. Die Initiative befürchtet, diese Regelung könnte die Anbieter von Kommunikationsdiensten zwingen, die Sicherheit und Integrität ihrer eigenen Dienste einzuschränken, um Nachrichtendiensten bei der Spionage zu unterstützen.

Wir fragen den Senat:

I. Einsatz für Zwecke der Strafverfolgung

1. Wie oft und aufgrund welcher Anlassstraftaten wurden in Bremen und Bremerhaven seit 2017 Maßnahmen der Quellen-Telekommunikationsüberwachung nach § 100a Absatz 1 Satz 2 und 3 oder der Online-Durchsuchung nach § 100b der Strafprozessordnung

a) von der Staatsanwaltschaft beantragt,

b) richterlich angeordnet,

c) wegen Gefahr in Verzug von der Staatsanwaltschaft angeordnet?

d) tatsächlich durchgeführt?

Bitte Quellen-TKÜ und Online-Durchsuchung getrennt ausweisen und jeweils nach Kalenderjahren aufschlüsseln. Bei politisch motivierter Kriminalität bitte zusätzlich nach Phänomenbereich differenzieren.

2. In wie vielen dieser Fälle kam

a) die BKA-Eigenentwicklung RCIS,

b) FinSpy,

c) Pegasus,

d) eine andere Spionagesoftware

zum Einsatz?

3. Soweit angeordnete Maßnahmen der Quellen-TKÜ oder Online-Durchsuchung nicht erfolgreich durchgeführt wurden, aus welchen Gründen scheiterte dies?

4. Welche wesentlichen Ermittlungserfolge konnten von bremischen Strafverfolgungsbehörden seit 2017 durch Maßnahmen der Quellen-TKÜ oder der Online-Durchsuchung erzielt werden?

5. Auf wie viele unterschiedliche Varianten von Trojaner-Software von wie vielen Herstellern für welche Einsatzgebiete können die bremischen Strafverfolgungsbehörden im Bedarfsfall zurückgreifen?

6. Durch welche Stellen werden den bremischen Sicherheitsbehörden die technischen Mittel zur Durchführung von Quellen-TKÜ und Online-Durchsuchung zur Verfügung gestellt?

7. Inwieweit müssen die bremischen Strafverfolgungsbehörden beim praktischen Einsatz von Staatstrojanern auf die Unterstützung von Bundesbehörden (z. B. BKA, ZITIS) oder anderen Stellen zurückgreifen?

8. Die Anwendung welcher der folgenden bekannten Methoden, um einen Staatstrojaner heimlich auf dem Gerät einer beschuldigten Person zu installieren, dürfen die bremischen Strafverfolgungsbehörden unter welchen Voraussetzungen veranlassen:

a) Aufspielen im Rahmen von Sicherheitskontrollen, etwa an Flughäfen,

b) heimliches Betreten von Wohnungs- oder Geschäftsräumen,

c) heimliches Entwenden und Zurücklegen des Geräts, auch unter Inanspruchnahme von Vertrauenspersonen,

d) Aufspielen als versteckter Bestandteil von Software, zu deren Nutzung die beschuldigte Person durch andere Behörden verpflichtet oder angehalten wird (Corona-Warn-App, CovPass, ELSTER, AusweisApp2, NINA, Katwarn, Mängelmelder etc.),

e) Aufspielen durch eine E-Mail oder Nachricht an eine nur von der beschuldigten Person genutzten Zieladresse,

f) Aufspielen durch eine E-Mail oder Nachricht an eine möglicherweise auch von anderen Personen genutzte Zieladresse?

9. Welche Umstände hindern die bremischen Strafverfolgungsbehörden daran, Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung häufiger als bisher einzusetzen?

10. Wie bewertet der Senat die bisher erreichte Einsatzfähigkeit von Quellen-TKÜ und Online-Durchsuchung und ihren effektiven Nutzen für die Strafverfolgung?

11. Wie bewertet der Senat die Koalitionsvereinbarung von SPD, Grünen und FDP auf Bundesebene, die Eingriffsschwelle für den Einsatz von Überwachungssoftware zur Quellen-TKÜ an die Vorgaben des Bundesverfassungsgerichts für die Online-Durchsuchung anzupassen, also den Einsatz auf besonders schwere Straftaten zu begrenzen?

II. Einhaltung verfassungsrechtlicher Vorgaben

12. Welche Stellen sind dafür verantwortlich zu gewährleisten, dass die den bremischen Strafverfolgungsbehörden zur Verfügung stehenden Staatstrojaner den verfassungsrechtlichen Vorgaben genügen, indem tatsächlich und nicht etwa nur scheinbar technisch sichergestellt ist, dass

a) an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,

b) die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden,

c) der eingesetzte Staatstrojaner nach dem Stand der Technik gegen unbefugte Nutzung geschützt ist,

d) im Falle der Quellen-TKÜ ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird?

13. Welche Erkenntnisquellen (Quellcodes, Audits, Zertifikate etc.) stehen den zuständigen Stellen zur Verfügung, um prüfen zu können, ob die verfassungsrechtlichen Vorgaben eingehalten werden?

14. Sind die bremischen Sicherheitsbehörden berechtigt, alle vorliegenden Informationen über die ihnen für den Einsatz zur Verfügung stehenden Staatstrojaner an das Gericht bzw. G 10-Kontrollgremium herauszugeben, das für die Anordnung oder rechtliche Überprüfung der Maßnahme zuständig ist?

15. Sind die bremischen Sicherheitsbehörden berechtigt, alle vorliegenden Informationen über die ihnen für den Einsatz zur Verfügung stehenden Staatstrojaner an andere öffentliche Stellen herauszugeben, die über die erforderlichen Kompetenzen verfügen, um die Einhaltung der verfassungsrechtlichen Vorgaben überprüfen zu können (z. B. an das Bundesamt für Sicherheit in der Informationstechnik)?

16. Geht der von bremischen Strafverfolgungsbehörden veranlasste Einsatz von Staatstrojanern mit Geheimhaltungsverpflichtungen oder -zusagen einher, die geeignet sind, die parlamentarische Kontrolle dieser Einsätze durch die Bürgerschaft einzuschränken? Wenn ja, welche Verpflichtungen oder Zusagen sind dies und wem gegenüber gelten sie?

III. IT-Sicherheit und Schwachstellen

17. Welche potentiellen Schäden für kritische Infrastrukturen, Behörden, Unternehmen, Privathaushalte und Umwelt drohen durch Cyberangriffe mit Schadsoftware, wenn hierbei offene Schwachstellen in weit verbreiteten Betriebssystemen ausgenutzt werden können? Welche durch Ransomware-Attacken bereits entstandenen Schäden für bremische Behörden oder Unternehmen sind dem Senat bekannt?

18. Welche Konsequenzen haben deutsche und internationale Sicherheitsbehörden nach Kenntnis des Senats nach den Attacken mit dem sogenannten WannaCry-Trojaner im Hinblick auf die Geheimhaltung von Sicherheitslücken gezogen?

19. Wie hoch bewertet der Senat die Gefahr, dass Zielpersonen, die einen Staatstrojaner auf ihrem Gerät entdecken, die Funktionsweise des Staatstrojaners analysieren und für kriminelle Zwecke nutzen, und welche Sicherheitsvorkehrungen bestehen, um dies zu verhindern?

20. Nutzen die Staatstrojaner, die den bremischen Sicherheitsbehörden zur Verfügung stehen, nach Kenntnis des Senats IT-Schwachstellen aus, welche die Integrität der von vielen Unternehmen und Menschen im Land Bremen verwendeten IT-Produkte bedrohen können, und was unternimmt der Senat, um auf eine Schließung dieser Sicherheitslücken hinzuwirken?

21. Hält der Senat es für vertretbar, mit Hilfe von Staatstrojanern IT-Sicherheitslücken auszunutzen und diese Schwachstellen gegenüber den betroffenen IT-Herstellern geheim zu halten, obwohl sie mit unabsehbaren Folgen auch von kriminellen Personen ausgenutzt werden könnten?

22. Welche Konsequenzen aus der Entscheidung des Bundesverfassungsgerichts vom 8. Juni 2021 zur staatlichen Nutzung von IT-Sicherheitslücken wurden von den deutschen und den bremischen Sicherheitsbehörden gezogen?

a) Durch welche Stellen ist gegebenenfalls die vom Bundesverfassungsgericht geforderte Abwägung zwischen den Gefahren für die allgemeine IT-Sicherheit, die durch eine von Staatstrojanern ausgenutzte Sicherheitslücke verursacht werden, und dem Nutzen, der durch den Einsatz der Staatstrojaner erzielt werden kann, in Bezug auf die Staatstrojaner, die den bremischen Strafverfolgungsbehörden zur Verfügung stehen, mit welchen Ergebnissen durchgeführt worden?

b) Wurde vor dem Einsatz eines Staatstrojaners durch bremische Sicherheitsbehörden insbesondere eine Datenschutz-Folgenabschätzung gemäß § 67 des Bundesdatenschutzgesetzes durchgeführt bzw. wurde dies nachgeholt, nachdem das Bundesverfassungsgericht in seiner Entscheidung vom 8. Juni 2021 darauf hinwies, dass eine Datenschutz-Folgenabschätzung vor dem Einsatz von Überwachungssoftware im Rahmen einer Quellen-TKÜ zweifellos durchzuführen sei? Wenn ja, welche wesentlichen Ergebnisse sind aus der Datenschutz-Folgenabschätzung und ggf. aus der Anhörung der Landesbeauftragten für Datenschutz und Informationssicherheit hervorgegangen?

23. Welche Maßnahmen werden unternommen, um in deutschen Sicherheitsbehörden und bei den Lieferanten der von ihnen verwendeten Staatstrojaner etwaigen Fehlanreizen entgegenzuwirken, gemeingefährliche Sicherheitslücken nicht den betroffenen Herstellern zu melden, weil sie für den effektiven Einsatz von Staatstrojanern ausgenutzt werden sollen?

24. Wie bewertet der Senat die Bedeutung einer sicheren Verschlüsselung von elektronischer Kommunikation für

a) die Pressefreiheit und den Quellenschutz,

b) oppositionelle Kräfte und diskriminierte Minderheiten in Staaten mit politischer Verfolgung,

c) Wirtschaftsunternehmen in Bremen und Bremerhaven?

25. Sind die Sicherheitslücken im iOS-Betriebssystem, durch die der Pegasus-Trojaner mit dem bloßen Empfang einer iMessage installiert und aktiviert werden konnte (Zero-Click-Attacke), nach Kenntnis des Senats mittlerweile vollständig geschlossen? Welche Auswirkungen auf die dienstliche Verwendung von iPhones und iPads im Verantwortungsbereich des Senats hat dieser Sachverhalt?

IV. Staatstrojaner für den Verfassungsschutz

26. In seinem Urteil vom 15. Dezember 1970 zur Frage, ob der Bundesgesetzgeber zum Erlass des Gesetzes zu Artikel 10 Grundgesetz befugt war, meinte das Bundesverfassungsgericht, die Gesetzgebungskompetenz des Bundes für Regelungen über die Überwachung des Brief-, Post- und Fernmeldeverkehrs durch Landesverfassungsschutzbehörden ergebe sich aus der Zuständigkeit für das gerichtliche Verfahren (Artikel 74 Absatz 1 Nummer 1), da die Maßnahmen wenigstens mittelbar der Verhinderung, Aufklärung und Verfolgung von Straftaten dienten. Hält der Senat diese Annahme angesichts der späteren Rechtsprechung des Bundesverfassungsgerichts zur Abgrenzung der Gesetzgebungskompetenzen für die Verfolgung von Straftaten einerseits und der Abwehr von Gefahren sowie der Verhütung von Straftaten andererseits noch für tragfähig?

27. Inwieweit ermächtigt die ausschließliche Gesetzgebungskompetenz für die Zusammenarbeit des Bundes und der Länder auf dem Gebiet des Verfassungsschutzes (Artikel 73 Absatz 1 Nummer 10 Buchstabe b des Grundgesetzes) den Bund zur Regelung von Eingriffsbefugnissen der Landesverfassungsschutzbehörden?

28. Bestehen nach Ansicht des Senats Zweifel an der Vereinbarkeit der Regelung in § 11 Absatz 1a des Artikel-10-Gesetzes mit der grundgesetzlichen Gesetzkompetenzverteilung zwischen Bund und Ländern? Bitte begründen.

29. Inwieweit ist der bremische Landesgesetzgeber berechtigt, die für das Landesamt für Verfassungsschutz nach dem Artikel-10-Gesetz bestehenden Befugnisse zu erweitern, zu konkretisieren, einzuschränken oder aufzuheben, etwa durch eine Änderung von § 8 Absatz 1 Nummer 11 des Bremischen Verfassungsschutzgesetzes?

30. Welche der folgenden bekannten Methoden, um einen Staatstrojaner heimlich auf dem Gerät einer Zielperson zu installieren, darf das Bremer Landesamt für Verfassungsschutz aufgrund der in § 2 Absatz 1a Satz 1 Nummer 4 des Artikel-10-Gesetzes geregelten Pflicht zur Umleitung von Telekommunikation unter welchen Voraussetzungen veranlassen:

a) Manipulation oder Fälschung von Webseiten,

b) Manipulation oder Fälschung von Software-Updates,

c) Manipulation oder Fälschung von SSL/TLS-Zertifikaten,

d) Manipulation oder Fälschung von Software-Signaturen?

31. Wie bewertet der Senat die Bedeutung des Vertrauens der Menschen in die Integrität von Sicherheitsupdates, von SSL/TLS-Zertifikaten und von Software-Signaturen für die allgemeine IT-Sicherheit?

32. Wie bewertet der Senat die Koalitionsvereinbarung von SPD, Grünen und FDP auf Bundesebene, die Eingriffsschwelle für den Einsatz von Überwachungssoftware zur Quellen-TKÜ an die Vorgaben des Bundesverfassungsgerichts für die Online-Durchsuchung anzupassen, den Einsatz also

auch für Verfassungsschutzbehörden auf die Abwehr einer mindestens konkretisierten Gefahr im polizeilichen Sinne für ein besonders gewichtiges Rechtsgut zu beschränken?

V. Alternativen zu Staatstrojanern

33. Inwieweit nutzen die bremischen Strafverfolgungsbehörden die Möglichkeit, über die Anbieter von Messenger-Apps an Metadaten der verschlüsselten Kommunikation zu gelangen und welche rechtlichen und tatsächlichen Herausforderungen haben sich dabei gezeigt?

34. Inwieweit nutzt die Polizei die nach dem Bremischen Polizeigesetz bestehende Möglichkeit, Smartphones sicherzustellen, um zum Zwecke der Gefahrenabwehr Zugriff auf die auf dem Gerät enthaltenen Daten zu erlangen?

35. Welche gesetzgeberischen, regulatorischen oder sonstigen Versuche der Einwirkung auf die Hersteller von Betriebssystemen und Messengerdiensten mit dem Ziel, eine Installation von technischen Mitteln zur Ausleitung von Daten auf Geräten einer Zielperson ohne das Ausnutzen von den Herstellern unbekannten Schwachstellen zu ermöglichen, sind dem Senat bekannt?

36. Wie bewertet der Senat – im Vergleich zu Staatstrojanern – die Praktikabilität von schonenderen, weil ohne den Einsatz von Staatstrojanern möglichen Methoden der Quellen-Telekommunikationsüberwachung, wie etwa den Zugriff auf die Telekommunikation der Zielperson über Whatsapp Web/Desktop, Telegram Cloud oder Signal Desktop?

37. Wie bewertet der Senat den Vorschlag, die Hersteller von Messenger-Apps und Betriebssystemen zu verpflichten, im Einzelfall auf richterliche Anordnung bestimmten Zielpersonen eine App-Version mit Backdoor oder deaktivierter Verschlüsselung aufzuspielen, um so Zugriff auf die Kommunikation zu erhalten, ohne die Integrität der Verschlüsselung auf anderen Geräten zu beeinträchtigen oder Sicherheitslücken auszunutzen?

38. Wie bewertet der Senat die am 6. November 2020 erhobene Forderung des EU-Ministerrats, den Anbietern sicherer Kommunikationslösungen die Pflicht aufzuerlegen, Hintertüren für staatliche Stellen einzurichten, insbesondere auch in Bezug auf die Auswirkungen für die allgemeine IT-Sicherheit?

39. Wie bewertet der Senat die in dem Verordnungsentwurf der Europäischen Kommission vom 11. Mai 2022 enthaltene Verpflichtung für Anbieter von Ende-zu-Ende-verschlüsselter Kommunikation (wie Signal, Threema oder WhatsApp), auf Anordnung die unverschlüsselten Kommunikationsinhalte auf dem Gerät auf Abbildungen von Kindesmissbrauch sowie

sogenanntes „Grooming“ zu scannen und ggf. an staatliche Behörden auszuleiten?

40. Wie bewertet der Senat die Forderung des Europäischen Datenschutzbeauftragten nach einem in der gesamten Europäischen Union geltenden Verbot der Entwicklung und des Einsatzes von Ausspähsoftware wie Pegasus sowie die darüber hinaus gehende Forderung von zivilgesellschaftlichen Organisationen, den Vertrieb und Einsatz von Staatstrojaner international zu ächten und zu sanktionieren?

Beschlussempfehlung:

Björn Fecker und Fraktion BÜNDNIS 90/DIE GRÜNEN