Antwort auf eine Große Anfrage
- Drucksache 16/4116 -

Wortlaut der Großen Anfrage der Fraktion DIE LINKE vom 19.10.2011

Quellen-Telekommunikationsüberwachung und Onlinedurchsuchungen - Wie steht es mit dem Einsatz von Staats-Trojanern in Niedersachsen?

Der Chaos Computer Club (CCC) hat am 8. Oktober 2011 ein Papier veröffentlicht, in dem er Software analysiert, die sich auf Festplatten von Rechnern aus mehreren Bundesländern befand. In seiner Analyse führt der CCC aus, dass die offensichtlich staatlicherseits aufgespielte und genutzte Software eine sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) ermöglicht, aber auch weit darüber hinaus genutzt werden kann und außerdem erhebliche Sicherheitsmängel aufweist. Insbesondere sei es möglich, jederzeit über eine Onlineverbindung Programmcode nachzuladen und damit weitere Funktionen, z. B. zur Raumüberwachung über die Webcam des Computers oder zur Aufzeichnung von Tastaturanschlägen oder Bildschirminhalten, zu aktivieren.

Mit seinem Urteil vom 27. Februar 2008 zu Onlinedurchsuchungen hat das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht abgeleitet, das sich aus Artikel 2 Abs. 1 GG in Verbindung mit Artikel 1 Abs.1 GG ergibt.

Das Bundesverfassungsgericht beschreibt in seinem Urteil die weite Verbreitung informationstechnischer Systeme im Alltag und die deutlich gestiegene Bedeutung dieser Systeme für die Persönlichkeitsentfaltung. Es beschreibt auch die Vielzahl der Nutzungsmöglichkeiten durch die Anwender und dass neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen bestehen. Es legt dar, dass sich aus diesen Möglichkeiten und Gefahren ein erhebliches grundrechtliches Schutzbedürfnis ergibt, dem die bisherigen grundrechtlichen Bestimmungen wie auch die bis dahin in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen nicht hinreichend Rechnung trugen.

Das Bundesverfassungsgericht erläutert in seinem Urteil, dass mit der Infiltration eines informationstechnischen Systems zum Zweck der Telekommunikationsüberwachung die entscheidende Hürde genommen ist, um das System insgesamt auszuspähen. Es zeigt auch die dadurch bedingte Gefährdung auf, dass Daten zur Kenntnis genommen werden können, die keinen Bezug zur telekommunikativen Nutzung des Systems haben, und erwähnt als Beispiele solcher nicht kommunikationsbezogenen Daten die Inhalte angelegter Dateien, die Aufrufhäufigkeit bestimmter Dienste bis hin zu Daten, die Rückschlüsse auf das Verhalten in der eigenen Wohnung zulassen. Als Schlussfolgerung führt das Bundesverfassungsgericht u. a. in seiner Pressemitteilung zum Urteil aus: „Angesichts der Schwere des Eingriffs ist die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.“ Das Bundesverfassungsgericht hat also bereits im Februar 2008 einen sehr engen Rahmen für Onlinedurchsuchungen gesteckt und insbesondere auch die Abgrenzung zwischen Quellen-TKÜ und Onlinedurchsuchung vorgenommen. Es hat ausgeführt, dass für die Durchführung von Quellen-TKÜ-Maßnahmen durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt werden müsse, dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt, damit in den Kernbereich der privaten Lebensführung nicht unzulässig eingegriffen wird.

Nach Aussagen des niedersächsischen Innenministers wurde in Niedersachsen bisher zweimal Trojaner-Software zur Quellen-TKÜ eingesetzt.

Wir fragen die Landesregierung:

I. Einsatz von Trojaner-Software

1. Von welchen Behörden und Dienststellen des Landes Niedersachsen und von welchen von ihnen beauftragten Unternehmen wurde bisher Trojaner-Software eingesetzt?
2. In wie vielen Fällen und für welche Zeiträume erfolgte jeweils der Einsatz?
3. Welche Art der Kommunikation wurde jeweils überwacht?
4. Wurden bzw. werden bei den bisherigen Einsätzen von Trojaner-Software durch Behörden oder Dienststellen des Landes Niedersachsen oder von ihnen beauftragte Unternehmen jeweils nur Kommunikationsinhalte ermittelt oder auch weitere Daten (z. B. Bildschirminhalte, Tastenanschläge, Web-Cam- oder Mikrofonaufnahmen, gespeicherte Dateien, gegebenenfalls andere Daten)?
5. Auf welcher Rechtsgrundlage erfolgten die jeweiligen Einsätze von Trojaner-Software?
6. Auf welchem Wege wurde die Software jeweils auf die zu überwachenden Computer gespielt?
7. Da bereits mit dem Aufspielen von Trojaner-Software zwangsläufig die Veränderung von Festplatteninhalten und Funktionsweise des betreffenden Systems verbunden ist und diese Maßnahme also über einen nur beobachtenden, lesenden Zugriff hinausgeht: Auf welcher Rechtsgrundlage erfolgten diese Veränderungen von Festplatteninhalten und Funktionsweisen von Computersystemen jeweils?
8. Von welchen Behörden und Dienststellen des Landes Niedersachsen und von welchen von ihnen beauftragten Unternehmen wurde bisher erfolglos der Versuch unternommen, Trojaner-Software einzusetzen?
9. In wie vielen Fällen und wann erfolgten solche nicht erfolgreichen Versuche?
10. Welche Art der Kommunikation sollte bei diesen erfolglosen Versuchen überwacht werden?
11. War bei diesen erfolglosen Versuchen über das Abgreifen von Telekommunikationsinhalten hinaus das Abgreifen weiterer Daten geplant, wenn ja, welcher Art von Daten?
12. Auf welcher Rechtsgrundlage erfolgten die erfolglosen Versuche dieser Trojaner-Einsätze?
13. Auf welchem Wege wurde bei diesen erfolglosen Versuchen versucht, die Software auf die Computer zu spielen?
14. Da bereits mit dem Aufspielen von Trojaner-Software zwangsläufig die Veränderung von Festplatteninhalten und Funktionsweise des betreffenden Systems verbunden ist und diese Maßnahme also über einen nur beobachtenden, lesenden Zugriff hinausgeht: Auf welcher Rechtsgrundlage wurden diese Veränderungen von Festplatteninhalten und Funktionsweisen von Computersystemen jeweils versucht?
15. Welche vermuteten Straftaten bzw. welche Gefahren waren jeweils die konkreten Anlässe für die Durchführung oder den Versuch des Einsatzes von Trojaner-Software?
16. a) Wurden an Behörden oder Dienststellen des Landes Niedersachsen Rechtshilfegesuche anderer Staaten, beispielsweise der Niederlande, gestellt, nach denen Rechner außerhalb Deutschlands mit Trojaner-Software überwacht werden sollten?

    b) Wenn ja, wurde diesen Rechtshilfegesuchen jeweils entsprochen, oder wurden sie abgelehnt?
17. Hat es umgekehrt Rechtshilfegesuche aus Niedersachsen an Behörden oder Dienststellen anderer Staaten gegeben mit dem Ziel, Rechner in Niedersachsen zwecks Quellen-TKÜ oder Onlinedurchsuchungen zu infiltrieren?

18. Wurden an Behörden oder Dienststellen des Landes Niedersachsen Rechtshilfegesuche anderer Bundesländer gestellt, nach denen Rechner außerhalb Niedersachsens mit Trojaner-Software überwacht werden sollten? Wenn ja, wurde diesen Rechtshilfegesuchen jeweils entsprochen, oder wurden sie abgelehnt?

19. Hat es umgekehrt Rechtshilfegesuche aus Niedersachsen an Behörden oder Dienststellen anderer Bundesländer oder an Behörden oder Dienststellen des Bundes gegeben mit dem Ziel, Rechner in Niedersachsen zwecks Quellen-TKÜ oder Onlinedurchsuchungen zu infiltrieren?

II. Erwerb, Anmietung und Eigenentwicklung von Trojaner-Software

20. Wann und von welchen Firmen wurde von Behörden oder Dienststellen des Landes Niedersachsen Trojaner-Software erworben?

21. a) Gab es vor der Entscheidung für Kauf oder Anmietung von Trojaner-Software durch Behörden oder Dienststellen des Landes Niedersachsen eine Ausschreibung?

    b) Wenn ja, mit welchem konkreten Inhalt, und war die Ausschreibung öffentlich?

22. Wie hoch sind bzw. waren jeweils die Beträge für Kauf oder Miete der Software, mit dem Einsatz verbundene Dienstleistungen der Lieferanten und die Bereitstellung der Infrastruktur für die Einsätze?

23. Da Software der Firma DigiTask eingesetzt wurde: Wie bewertet die Landesregierung die Seriosität des Unternehmens DigiTask vor dem Hintergrund der Tatsache, dass laut einem Onlineartikel der *Wirtschaftswoche* vom 23. Juni 2008 das mit DigiTask verbundene Unternehmen Reuter Electronic im Jahr 2002 rechtskräftig wegen Bestechung und Vorteilsgewährung verurteilt wurde, nachdem Reuter erhebliche Summen an das Kölner Zollkriminalamt gezahlt hatte und dieses im Gegenzug bevorzugt DigiTask-Geräte erwarb?

24. Wie bewertet die Landesregierung im Hinblick auf das Vertrauen der Bürgerinnen und Bürger die Tatsache, dass Niedersachsen Trojaner-Software von einem Unternehmen bezieht, das 2009 mit dem Big Brother Award der Kategorie Wirtschaft ausgezeichnet wurde, der von der Bürgerrechtsorganisation Foebud an Unternehmen verliehen wird, „die in auffallender Weise den Datenschutz verletzen oder missachten“?

25. Da der Innenminister im Landtag und gegenüber Medien ausgeführt hat, dass ein Wechsel weg von der Firma DigiTask und hin zu einem anderen Lieferanten erfolgt ist bzw. entsprechende Qualitätssicherungsmaßnahmen gerade laufen:

    a) Welche Gründe haben konkret zur Abkehr vom Lieferanten DigiTask geführt?

    b) Handelt es sich bei dem neuen Lieferanten um die Firma Syborg?

    c) Wenn ja, ist der Landesregierung bekannt, dass Syborg eine Tochterfirma der Firma Verint Systems ist?

    d) Falls ja, sind der Landesregierung Skandale bekannt, in denen die Fima Verint Systems eine Rolle spielte?

    e) Falls der neue Lieferant für Trojaner-Software nicht Syborg ist, welcher ist es dann?

26. a) Hat das Land Niedersachsen Software zur Quellen-TKÜ oder für Onlinedurchsuchungen selbst entwickelt?

    b) Wenn ja, durch welche Behörden oder Dienststellen?

    c) Welche Maßnahmen sind erfolgt, um die Einhaltung rechtlicher Vorgaben und die Verfassungskonformität der entwickelten Software sicherzustellen?

III. Prüfung von Qualität und Rechtmäßigkeit eingesetzter Trojaner-Software

27. Wie wurde und wird jeweils sichergestellt, dass die für Quellen-TKÜ oder Onlinedurchsuchungen von Behörden oder Dienststellen des Landes Niedersachsen oder von ihnen beauftragter Unternehmen eingesetzte Software gesetzes- und verfassungskonform ist und insbesondere den Vorgaben des Bundesverfassungsgerichtsurteils zu Onlinedurchsuchungen vom 27. Februar 2008 genügt?

28. a) Wurde vor Einsatz von Trojaner-Software der Sourcecode von Landesmitarbeiterinnen oder Landesmitarbeitern gesichtet und hinsichtlich Recht- und Verfassungsmäßigkeit bewertet?

    b) Falls nein, warum nicht?

    c) Falls ja, mit welchem Ergebnis, und wie wurde sichergestellt, dass der gesichtete Sourcecode tatsächlich die Quelle für die Kompilierung der dann eingesetzten Software war?

29. a) Durch welche Firmen, Einrichtungen oder Behörden wurde die Software vor Einsatz jeweils überprüft?

    b) Hat es insbesondere wie in Bayern eine Überprüfung ausschließlich durch Landeskriminalämter anderer Länder gegeben?

30. Nachdem in Werbeunterlagen der Firma DigiTask (siehe http://cryptome.org/0005/michael thomas.pdf) ausdrücklich auf die Möglichkeit hingewiesen wird, dass ihre Software jederzeit online aktualisiert, also durch Nachladen von Code geändert oder erweitert werden kann:

    a) War diese Funktion bekannt?

    b) Wenn nicht, warum nicht, nachdem DigiTask damit offenbar sogar wirbt?

    c) Hat es im Rahmen der Überprüfung der Funktionsweise der Software vor ihrem Einsatz eine Bewertung dieser Aktualisierungsmöglichkeit und der damit verbundenen Risiken und möglichen Grundrechtsbeeinträchtigungen gegeben?

    d) Wenn ja, mit welchem Ergebnis?

    e) Wenn nein, warum nicht?

31. Nachdem in Werbeunterlagen der Firma DigiTask (siehe http://cryptome.org/0005/michael thomas.pdf) unter dem Punkt „What is provided by the DigiTask solution?“, Unterpunkt „Data Analysis“ ausdrücklich der Punkt „Core area of private life“, also „Kernbereich der privaten Lebensführung“ erwähnt wird:

    a) Hat die Landesregierung bzw. haben die ihr nachgeordneten, die Trojaner-Software einsetzenden Behörden oder Dienststellen hinterfragt und geprüft, inwieweit hier verfassungswidrige Eingriffe möglich sind oder der Einsatz der Software das Risiko birgt, dass diese geschehen?

    b) Wurde von der Firma DigiTask eine Zusicherung gefordert, dass verfassungswidrige Eingriffe mithilfe der Software nicht erfolgen können?

    c) Hat die Firma DigiTask eine solche Zusicherung abgegeben?

    d) Wenn nicht, warum wurde die Software dennoch eingesetzt?

32. Da der CCC in seiner Analyse der Software der Firma DigiTask ausführt „Das Sicherheitsniveau dieses Trojaners ist nicht besser, als würde er auf allen infizierten Rechnern die Passwörter auf '1234' setzen“:

    a) Sind der Landesregierung bzw. den Behörden und Dienststellen des Landes Niedersachsen, die die Software einsetzten bzw. einsetzen, die vom CCC aufgeführten Sicherheitslücken bekannt?

b) Ist die Software hinreichend gegen Eingriffe von außen geschützt oder besteht ein hohes Risiko der Manipulation der vermeintlich korrekt erhobenen Daten?

c) Macht die Software die infiltrierten Rechner anfällig für weitere Angriffe von außen, die mit der Überwachung nichts zu tun haben?

d) Bringt der Einsatz der Software das Risiko mit sich, den Rechner in seiner Funktionsfähigkeit zu beeinträchtigen, also zu beschädigen?

33. Wie bewertet die Landesregierung die sich zwangsläufig mit der Überwachung eines überwachten Kommunikationspartners ergebende inhaltliche Mitüberwachung des anderen, nicht überwachten Kommunikationspartners bei der Quellen-TKÜ?

34. Da der Geheimdienstkoordinator im Bundeskanzleramt, Günter Heiß, der Presse gegenüber ausführte, dass die Landeskriminalämter zur Telekommunikationsüberwachung „multifunktionale Rohlinge“ kaufen würden, die jedes Mal auf das Ziel und den Überwachungszweck zugeschnitten werden müssten:

a) Wer ist in Niedersachsen für diese Softwarekonfigurationstätigkeit bei Einsatz von Trojaner-Software zuständig?

b) Wer hat diese Aufgabe bei bisherigen erfolgreichen und erfolglosen Einsätzen von Trojaner-Software durchgeführt?

c) Wie wurde bzw. wird diese Tätigkeit daraufhin überwacht, dass die Einhaltung rechtlicher Vorgaben und die Verfassungsmäßigkeit gewährleistet sind?

d) Wurde der Landesdatenschutzbeauftragte jeweils eingebunden und in welcher Form und mit welchem Ergebnis?

35. Welche Funktionen kann bzw. konnte die von niedersächsischen Behörden und Dienststellen und von ihnen beauftragten Unternehmen eingesetzte Trojaner-Software über die reine Quellen-TKÜ hinaus ausführen, unabhängig davon, ob diese Funktionen tatsächlich ausgeführt werden oder wurden?

36. Da die DigiTask-Software durch Befehle (Zahlencodes plus Parameter) von außen steuerbar ist:

a) Wer hatte bzw. hat jeweils in den bisherigen Einsatzfällen die Möglichkeit, solche Steuerungsbefehle abzusetzen?

b) Welche Maßnahmen wurden ergriffen, um zu verhindern, dass Unbefugte solche Befehle an die Trojaner-Software auf dem infiltrierten System senden?

37. Wurde bei den bisherigen Einsatzfällen von DigiTask-Software die Nachladefunktion genutzt, und, wenn ja, was wurde jeweils nachgeladen?

IV. Datenschutz und Datensicherheit

38. a) Wurden bzw. werden beim Einsatz von Software zur Quellen-TKÜ durch Behörden oder Dienststellen des Landes Niedersachsen oder von ihnen beauftragte Unternehmen die ermittelten Daten an Serversysteme in den USA gesendet?

b) Wenn ja, von welchem Unternehmen werden diese Server betrieben?

39. Soweit die ermittelten Daten an Serversysteme in den USA gesendet wurden oder werden:

a) Wie bewertet die Landesregierung die Tatsachen, dass Mitarbeiterinnen und Mitarbeiter der Betreiberfirma der Server auf die Daten zugreifen könnten?

b) Wie bewertet die Landesregierung die Tatsache, dass aufgrund des sogenannten Patriot Act US-amerikanische Behörden berechtigt sind, auf Daten sämtlicher US-amerikanischen Firmen zuzugreifen und daher das laut § 4 b BDSG geforderte angemessene Datenschutzniveau bei einer Weiterleitung der Daten in die USA nicht gewährleistet ist?

40. Vor dem Hintergrund der Tatsache, dass als zu überwachende Telekommunikationsvorgänge vom niedersächsischen Innenminister wiederholt Skype-Telefonate genannt wurden:

    a) Wurde im jeweiligen Einzelfall erwogen, die entsprechenden Kommunikationsinhalte über die Firma Skype zu erhalten, um den Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme für die jeweils Betroffenen zu vermeiden?

    b) Wenn nicht, warum wurde dies nicht erwogen?

    c) Wenn ja, wurde dies versucht und mit welchem Ergebnis?

    d) Wenn nicht, warum nicht?

41. Vor dem Hintergrund, dass als zu überwachender Telekommunikationsvorgang vom niedersächsischen Innenminister wiederholt E-Mail genannt wurde:

    a) Wurde im jeweiligen Einzelfall erwogen, die entsprechenden Kommunikationsinhalte über die jeweiligen Serviceprovider zu erhalten, um den Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme für die jeweils Betroffenen zu vermeiden?

    b) Wenn nicht, warum wurde dies nicht erwogen?

    c) Wenn ja, wurde dies versucht und mit welchem jeweiligen Ergebnis?

    d) Wenn nicht, warum nicht?

42. Da der niedersächsische Innenminister in der Sendung „Phoenix-Runde“ am 13. Oktober 2011 ausführte, dass die Landesdatenschutzbeauftragten „im Vorfeld eingebunden“ würden, diese also „auf das Verfahren im Vorfeld draufschauen“ könnten:

    a) Wurde der niedersächsische Landesdatenschutzbeauftragte im Vorfeld des Einsatzes von Trojaner-Software durch Behörden und Dienststellen des Landes Niedersachsen und von ihnen beauftragte Unternehmen eingebunden?

    b) Wenn ja, in welcher Form, und zu welchem Ergebnis kam der Landesdatenschutzbeauftragte?

    c) Wenn nein, warum nicht?

43. a) Wie bewertet die Landesregierung die Tatsache, dass durch den Einsatz von Trojaner-Software ohne Wissen der jeweils überwachten Person Daten Dritten zur Kenntnis gelangen, zu deren Geheimhaltung sich die überwachte Person verpflichtet hat (z. B. PIN für Onlinebanking oder vertrauliche Geschäftsdaten)?

    b) Wie bewertet die Landesregierung die Tatsache, dass Daten im Verfügungsbereich überwachter Personen ohne ihr Wissen und Zutun weitergegeben werden, hinsichtlich möglicher Haftungs- und Regressfolgen für die überwachte Person?

44. a) Wann und in welchem Umfang werden bzw. wurden Personen, die mittels Trojaner-Software überwacht wurden, über diesen Grundrechtseingriff informiert?

    b) Wann und in welchem Umfang werden bzw. wurden Personen, bei denen Trojaner-Software zur Überwachung eingesetzt werden sollte, der Versuch aber nicht erfolgreich war, über den vorgesehenen Grundrechtseingriff informiert?

    c) Wann und in welchem Umfang wird bzw. wurde der Landesdatenschutzbeauftragte über geplante, erfolgende und erfolgte Einsätze von Trojaner-Software informiert?

V. Gerichtliche Verwertbarkeit der ermittelten Daten

45. Wie bewertet die Landesregierung die gerichtliche Verwertbarkeit der aus Quellen-TKÜ mithilfe der Software der Firma DigiTask erhaltenen Daten vor dem Hintergrund der Tatsache, dass laut Analyse des CCC bei Einsatz dieser Software ohne größere Schwierigkeiten andere Per-

sonen als die zu überwachenden Kommunikationsdaten an den datenempfangenden C+C-Server senden können, die vorgeblich von der überwachten Person stammen und von den tatsächlich von der überwachten Person stammenden Daten dann nicht mehr zu unterscheiden sind?

46. Wie bewertet die Landesregierung die gerichtliche Verwertbarkeit der Ergebnisse einer denkbaren Festplattendurchsuchung eines im Anschluss an eine Quellen-TKÜ beschlagnahmten Rechners hinsichtlich der Tatsachen,

    a) dass laut Analyse des CCC der Einsatz der DigiTask-Software das Risiko mit sich bringt, dass Daten von außen auf die Festplatte der überwachten Person gespielt werden können und der Beweis, dass die Daten vom zu überwachenden Nutzer des Rechners stammen, unmöglich werden könnte,

    b) dass bereits das Aufspielen der Trojaner-Software auf das jeweilige Computersystem ein schreibender, also die Festplatteninhalte und Funktionsweise des Systems verändernder Zugriff ist,

    c) dass Beklagte in einem Verfahren argumentieren könnten, dass offensichtlich auf die Festplatte geschrieben wurde (anders kann die Trojaner-Software ja nicht installiert werden) und daher auf der Festplatte befindliche Daten nicht von ihnen, den Beklagten, stammen müssen, sondern ebenso gut von denjenigen auf die Festplatte geschrieben worden sein könnten, die die Trojaner-Software auf die Festplatte geschrieben haben?

VI. Grundsätzliche Verfassungsmäßigkeit von Trojaner-Software

47. Wie bewertet die Landesregierung die Tatsache, dass nach Ansicht von Experten ein verfassungsgemäßer Einsatz von Trojaner-Software zur Quellen-TKÜ nicht möglich ist, weil die vom Bundesverfassungsgericht geforderte trennscharfe technische Abgrenzung zur deutlich weitergehenden Onlinedurchsuchung nicht zu erreichen ist?

Antwort der Landesregierung

Niedersächsisches Ministerium
für Inneres und Sport
- P 23.20/23.21-01425/2-1 -

Hannover, den 06.03.2012

Das digitale Zeitalter hat die weltweite Kommunikation geradezu revolutioniert. Datenpakete erreichen in Sekundenbruchteilen jeden gewünschten Adressaten dieser Erde. Kommunikation über neue Medien wie Internet, E-Mails, Internet-Telefonie sind zum internationalen Standard geworden und aus dem Portfolio der täglichen Lebensgewohnheiten nicht mehr wegzudenken. Laut BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) telefonierten im Jahr 2011 mehr als 11 Millionen Bundesbürger über das Internet. Die Nutzerzahl ist weiter ansteigend.

Internet-Telefonie oder Voice-over-IP (VoIP) ist das Telefonieren über Computernetzwerke, welche nach Internetstandards aufgebaut sind. Im Unterschied zu klassischen Telefonaten werden keine dezidierten Leitungen geschaltet, sondern Sprache digitalisiert und in kleinen Datenpaketen transportiert. VoIP über Instant-Messenger wie z. B. Skype ist im Internet kostenfrei und findet vielfach mit verschlüsselten Systemen statt. Eine Dekodierung der Daten ist aufgrund des eingesetzten Verschlüsselungsalgorithmus nicht möglich.

Auch Straftäter nutzen verschlüsselte Kommunikationstechnologie. Strafverfolgungsbehörden und andere Sicherheitsbehörden sind deshalb ständig gefordert, sich diesen Entwicklungen anzupassen und entsprechende Lösungen vorzuhalten. Aus diesem Grund wird die sogenannte Quel-

len-Telekommunikationsüberwachung (Quellen-TKÜ) zur Bekämpfung der Schwerstkriminalität und soweit erforderlich auch zur Abwehr drohender Gefahren für hochrangige Rechtsgüter eingesetzt.

Das Bundesverfassungsgericht hat in seinem Urteil zur Onlinedurchsuchung vom 27.02.2008 (1 BvR 370/07 und 1 BvR 595/07) festgestellt, dass Artikel 10 Abs. 1 GG (Brief-, Post- und Fernmeldegeheimnis) der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer Quellen-TKÜ ist, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.

Gemäß § 100 a StPO, § 33 a Nds. SOG und §§ 1 und 3 Artikel 10-Gesetz (G 10) ist die Aufzeichnung und Überwachung der Telekommunikation zulässig, soweit die Überwachung zur Aufklärung bestimmter Straftaten oder Gefahren erforderlich und verhältnismäßig ist.

Die Quellen-TKÜ unterscheidet sich von der klassischen TKÜ dadurch, dass die Daten nach verdeckter Implementierung einer Überwachungssoftware am Endgerät (der „Quelle“) des Verdächtigen noch vor der Verschlüsselung bzw. nach ihrer Entschlüsselung erhoben werden. Von der Quellen-TKÜ deutlich abzugrenzen ist die Online-Durchsuchung. Hierbei handelt es sich um die mittels einer Überwachungssoftware ausgeführte gezielte und heimliche Suche nach auf der Festplatte gespeicherten Daten und deren Ausleitung. Diese Befugnis haben niedersächsische Behörden nicht.

Die nach der Veröffentlichung des Chaos Computer Clubs vom 08.10.2011 zum „Bundestrojaner“ der Firma DigiTask in Niedersachsen erhobenen und veröffentlichten Daten zur Quellen-TKÜ beziehen sich auf den Zeitraum nach dem Bundesverfassungsgerichtsurteil zur Onlinedurchsuchung vom 27.02.2008.

In Niedersachsen wurden durch die Polizei bislang ausschließlich Maßnahmen der Quellen-TKÜ auf der Grundlage der Strafprozessordnung durchgeführt.

Die Maßnahmen der Niedersächsischen Verfassungsschutzbehörde stehen unter einem besonderen Geheimhaltungsvorbehalt. Für diese bestünde bei einer detaillierten Beantwortung sämtlicher Fragen die Gefahr, dass Rückschlüsse auf die Nutzungsintensität des nachrichtendienstlichen Mittels und auf die technischen Fähigkeiten und Methoden der Verfassungsschutzbehörde gezogen werden könnten. Dadurch wäre es möglich, mittelbar auch Erkenntnisse über die Arbeitsweise der Niedersächsischen Verfassungsschutzbehörde zu gewinnen. Insbesondere eine Darstellung konkreter Verfahren verbietet sich, da anderenfalls die Gefahr bestünde, dass auch Rückschlüsse auf das konkrete Beobachtungsfeld des Verfassungsschutzes gezogen werden könnten und dadurch die erforderliche weitere Beobachtung in bestimmten Bereichen gefährdet oder gar unmöglich gemacht würde.

Um die Aufgabenerfüllung und die Arbeitsfähigkeit des Verfassungsschutzes und damit auch die Sicherheit des Landes nicht zu gefährden, können daher konkrete Fragestellungen teilweise nicht beantwortet werden. Bei einer Abwägung zwischen dem Informationsrecht der Abgeordneten des Landtages einerseits und den dargestellten negativen Folgen für die künftige Arbeit des Verfassungsschutzes sowie den zu befürchtenden Nachteilen für das Wohl des Landes andererseits ist den Geheimhaltungsinteressen im Einzelfall Vorrang einzuräumen.

Dem Informationsrecht des Landtages wurde insoweit nachgekommen, als zu dem Thema Quellen-TKÜ eine Unterrichtung des Ausschusses für Angelegenheiten des Verfassungsschutzes in vertraulicher Sitzung am 02.02.2012 stattgefunden hat.

Zur langfristigen Sicherung des unverzichtbaren Ermittlungsinstruments Quellen-TKÜ ist auf Ebene der nationalen Sicherheitsbehörden einvernehmlich beschlossen worden, die jeweils vorhandenen Softwarelösungen einer bundesweit vereinbarten Evaluierung auf der Grundlage einer standardisierten Leistungsbeschreibung und eines Qualitätssicherungsprozesses unter Einbindung eines unabhängigen Expertengremiums zu unterziehen.

Darüber hinaus ist die Entwicklung einer eigenen, staatlichen Software zur Durchführung von Quellen-TKÜ im „Kompetenzzentrum Informationstechnische Überwachung“ im Bundeskriminalamt vorgesehen. Niedersachsen hat seine Mitwirkung an dem im Aufbau befindlichen Kompetenzzentrum zugesagt.

Auf die Antworten zu den Mündlichen Anfragen Nr. 35, 36 und 59 in der Drucksache 16/4225 - vgl. Anlagen zum Stenografischen Bericht über die 124. Sitzung des Landtages am 09.12.2011 - wird ergänzend hingewiesen.

Zur Beantwortung der Großen Anfrage habe ich vom Landeskriminalamt Niedersachsen, den Generalstaatsanwaltschaften und den Oberlandesgerichten Niedersachsens Informationen einholen lassen.

Dies vorangestellt, beantworte ich die Fragen auf der Grundlage dieser Berichte im Namen der Landesregierung wie folgt:

I. Einsatz von Trojaner-Software

Für die Niedersächsische Verfassungsschutzbehörde wird zur Beantwortung der Fragen 1 bis 6 und 8 bis 15 auf die Vorbemerkungen verwiesen.

Zu 1:

Die Staatsanwaltschaften erfassen statistisch jede Telekommunikationsüberwachungsmaßnahme nach § 100 a StPO.

Ob diese Telekommunikationsüberwachungsmaßnahme jedoch standardmäßig mit Hilfe des Dienstanbieters oder mittels Einsatz einer Software als Quellen-TKÜ durchgeführt wird, spielt für die Erfassung keine Rolle. Angaben zu durchgeführten Maßnahmen der Quellen-TKÜ können daher nur auf Grundlage entsprechender Abfragen bei Polizei, Staatsanwaltschaften und Gerichten erfolgen.

Seit dem Urteil des Bundesverfassungsgerichts wurden Maßnahmen der Quellen-TKÜ im vorgenannten Zeitraum durchgeführt in einem Verfahren, welches die Staatsanwaltschaft Hannover mit der PD Lüneburg im Jahr 2009 geführt hat, in einem Verfahren der Staatsanwaltschaft Stade mit der PD Lüneburg aus dem Jahr 2011 und in einem weiteren Verfahren der Staatsanwaltschaft Hannover, in welchem diese gemeinsam mit der Zollfahndung des Bundes ermittelte.

Hinsichtlich früherer Quellen-TKÜ-Maßnahmen wird ergänzend auf die Antwort der Landesregierung auf die Mündliche Anfrage Nr. 32 des Angeordneten Heiner Bartling, SPD, in der Drucksache 15/4115, verwiesen (Stenografischer Bericht über die 130. Plenarsitzung des Landtages am 19.10.2007, Anlage 30).

Zu 2:

Im Ermittlungsverfahren der Staatsanwaltschaft Hannover war die Software am 16.05.2009 aufgespielt worden. Die Maßnahme endete am 23.06.2009 mit der Festnahme des Beschuldigten. In dem Verfahren der Staatsanwaltschaft Stade erfolgte der Einsatz im Zeitraum vom 15.02.2011 bis zum 15.04.2011.

Im Rahmen der bei der Staatsanwaltschaft Hannover gemeinsam mit dem Zollfahndungsamt geführten Ermittlungen wurde die Software im Zeitraum vom 20.05.2009 bis zum 08.06.2009 eingesetzt.

Zu 3:

Die Überwachungsmaßnahmen der Polizei und des Zolls betrafen ausschließlich die über Skype geführte Kommunikation.

Zu 4:

Auf die Antwort zu Frage 3 wird verwiesen. Die auf Antrag der Staatsanwaltschaften erlassenen richterlichen Anordnungen bezogen sich ausdrücklich und ausschließlich auf eine Erhebung der Telekommunikationsdaten.

Zu 5:

Die Maßnahmen der Landespolizei und des Zolls wurden ausschließlich auf der Grundlage des § 100 a StPO durchgeführt.

Zu 6:

Die Implementierung der Überwachungssoftware ist abhängig von dem im Einzelfall verwendeten informationstechnischen System des Betroffenen.

Weitergehende Informationen, insbesondere zum taktischen Vorgehen und zu handelnden Personen der Sicherheitsbehörden in konkreten Verfahren, entziehen sich der öffentlichen Erörterung im Rahmen der Beantwortung einer parlamentarischen Anfrage.

Das Bekanntwerden von operativen Möglichkeiten, Praktiken und genutzten Techniken der Sicherheitsbehörden kann laufende und künftige Ermittlungen erschweren oder unmöglich machen. Es bestünde die Gefahr, dass operative Fähigkeiten und Methoden der Sicherheitsbehörden bekannt würden und nicht mehr eingesetzt werden könnten. Die Arbeitsfähigkeit der Sicherheitsbehörden wäre dadurch stark beeinträchtigt. Daher müssen bei der Beantwortung dieser Frage das in Artikel 24 der Niedersächsischen Verfassung geregelte Fragerecht der Abgeordneten und die Auskunftspflicht der Landesregierung nach Güterabwägung zwischen dem Fragerecht der Abgeordneten und den dargestellten negativen Folgen zurückstehen. Die Landesregierung ist jedoch grundsätzlich bereit, im Rahmen einer vertraulichen Ausschusssitzung den Landtag darüber zu informieren.

Zu 7:

Die Überwachung der Kommunikation mittels Quellen-TKÜ erfolgte auf der Grundlage des § 100 a StPO. Das Aufspielen der Software auf den zu überwachenden Computer stellt eine Vorbereitungshandlung dar und ist als Annex von gemäß § 100 a StPO gedeckt (vgl. LG Hamburg, Beschluss vom 13.09.2010, 608 Qs 17/10).

Für die Niedersächsische Verfassungsschutzbehörde ist die Installation der Software zur Durchführung einer Quellen-TKÜ von der im G 10 enthaltenen Eingriffskompetenz als sogenannte Annexkompetenz mit umfasst. Die Installation/Implementierung der Software, mittels derer Telekommunikationsdateien ausgeleitet werden sollen, und die damit einhergehende Ergänzung von Festplatteninhalten ist technisch gesehen die einzige, aber zwingende Voraussetzung für die Durchführung einer Quellen-TKÜ.

Hierbei findet zwar ein Eingriff in das vom Betroffenen genutzte informationstechnische System statt, es werden jedoch keine Daten ausgeleitet, die in dem informationstechnischen System gespeichert sind.

Zu 8:

Bei den Polizeibehörden des Landes Niedersachsen hat es bisher keine erfolglosen Versuche gegeben, Software zur Durchführung der Quellen-Telekommunikationsüberwachung einzusetzen.

Zu 9 bis 14:

Auf die Antwort zu Frage 8 wird verwiesen.

Zu 15:

Anlassstraftaten in den Verfahren der Landespolizei waren der Verdacht des Raubes mit Todesfolge und der Verdacht des Handeltreibens mit Betäubungsmitteln in nicht geringer Menge.

Dem Verfahren der Zollfahndung lagen der Verdacht der gewerbs- und bandenmäßigen Steuerhinterziehung, des Schmuggels und der Hehlerei in Tateinheit mit der Bildung einer kriminellen Vereinigung sowie der Geldwäsche zugrunde.

Hierbei handelt es sich in allen Fällen um schwere Straftaten im Sinne des Kataloges in § 100 a Abs. 2 StPO.

Bezüglich durchgeführter Versuche wird auf die Antwort zu Frage 8 verwiesen.

Für die Niedersächsische Verfassungsschutzbehörde regelt § 3 Abs. 1 G 10 die Voraussetzungen zum Einsatz einer Überwachungssoftware im Rahmen einer TKÜ. Danach dürfen Beschränkungsmaßnahmen angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der im Straftatenkatalog des § 3 G 10 abschließend aufgeführten Straftaten

plant, begeht oder begangen hat. Gleiches gilt, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind.

Zu 16 a:

Ersuchen um Unterstützung bei der grenzüberschreitenden Überwachung von Computern mittels Quellen-TKÜ sind von ausländischen Behörden nicht an niedersächsische Behörden oder Dienststellen herangetragen worden.

Zu 16 b:

Entfällt.

Zu 17:

Ersuchen um Unterstützung bei der grenzüberschreitenden Überwachung von Computern mittels Quellen-TKÜ sind von niedersächsischen Behörden oder Dienststellen nicht an ausländische Behörden herangetragen worden. Onlinedurchsuchungen sind rechtlich nicht zulässig und wurden von niedersächsischen Behörden und Dienststellen nicht durchgeführt. Diese sind rechtlich auch nicht zulässig.

Zu 18:

Ersuchen um Unterstützung bei der Überwachung von Computern mittels Quellen-TKÜ sind von Behörden anderer Bundesländer nicht an Niedersachsen herangetragen worden.

Zu 19:

Ersuchen um Unterstützung bei der Überwachung von Computern mittels Quellen-TKÜ sind von Niedersachsen nicht an Behörden oder Dienststellen anderer Bundesländer oder des Bundes gestellt worden.

II. Erwerb, Anmietung und Eigenentwicklung von Trojaner-Software

Für die Niedersächsische Verfassungsschutzbehörde wird zur Beantwortung der Fragen 20 bis 22 auf die Vorbemerkungen verwiesen.

Zu 20:

Die in den Jahren 2009 und 2011 durch die Landespolizei und den Zoll erfolgten Maßnahmen der Quellen-TKÜ wurden mit jeweils angemieteten Softwarelösungen der Firma DigiTask durchgeführt.

Im Jahr 2010 erfolgte eine europaweite Ausschreibung zur Beschaffung einer neuen zentralen TKÜ-Systemtechnik für die Landespolizei. Integraler Bestandteil dieser Beschaffungsmaßnahme ist eine Systemtechnik zur Überwachung verschlüsselter Kommunikationsabläufe. Lieferant der zentralen TKÜ-Systemtechnik ist die Firma Syborg.

Zu 21 a:

Die in 2009 und 2011 angemieteten und zum Einsatz gebrachten Softwareprodukte der Firma DigiTask wurden nicht ausgeschrieben. Grundsätzliche Regelungen für das öffentliche Auftragswesen finden sich in der Vergabe- und Vertragsordnung für Leistungen, Teil A (VOL/A) und dem gemeinsamen Runderlass des Niedersächsischen Ministeriums für Wirtschaft, Arbeit und Verkehr, der Staatskanzlei und der übrigen Ministerien zum öffentlichen Auftragswesen (Nds. MBl. 2011, S. 898 f.). Demnach dürfen bis zu einer festgesetzten Wertgrenze von 50 000 Euro freihändige Vergaben durchgeführt werden.

Die zwischenzeitlich neu beschaffte zentrale TKÜ-Systemtechnik für die Landespolizei ist im Jahr 2010 europaweit ausgeschrieben worden.

Zu 21 b:

Die Ausschreibung der Landespolizei zur neuen zentralen TKÜ-Systemtechnik war öffentlich und erfolgte europaweit. Der Auftrag umfasste Lieferung, Installation, Konfiguration und Inbetriebnahme eines kompletten TKÜ-Systems (Hardware und Software) einschließlich Ausbildung/Schulung, Service/Support, Instandsetzung/Wartung. Integraler Bestandteil der Ausschreibung bzw. des erstellten Leistungsverzeichnisses war eine Systemtechnik zur Überwachung verschlüsselter Kommunikation.

Zu 22:

Die Kosten für die angemietete Software in den beiden Verfahren der Landespolizei betrugen insgesamt 36 975 Euro. Eine detaillierte Kostenaufstellung ist aus Gründen vertraglicher Beschränkungen nicht möglich.

Die Kosten im Zollverfahren wurden ausschließlich vom Bund getragen.

Zu 23 und 24:

Die Firma DigiTask gilt im Bereich der Kommunikationsüberwachung als renommiertes Unternehmen und unterliegt seit dem Jahr 2001 der Geheimschutzbetreuung des Bundesministeriums für Wirtschaft und Technologie. Im Rahmen dieser Betreuung werden Mitarbeiter und Strukturen der Firma im Hinblick auf den Umgang mit amtlich geheim zu haltenden Informationen (Verschlusssachen) überprüft.

Der Big Brother Award 2009 wurde allen deutschen Unternehmen verliehen, die Produkte zur Telekommunikationsüberwachung anboten. Einige Firmen, so auch DigiTask, wurden stellvertretend benannt. Nähere Hintergründe zur „Preisverleihung“ sind der Landesregierung nicht bekannt.

Die Landesregierung sieht keine Veranlassung, aufgrund einiger veröffentlichter Online-Artikel eine öffentliche Bewertung zur Seriosität einzelner Unternehmen vorzunehmen.

Zu 25 a:

Die Zusammenarbeit erfolgte jeweils anlassbezogen soweit entsprechende richterliche Anordnungen zur Überwachung der Telekommunikation vorlagen. Durch den Zuschlag an die Firma Syborg im Rahmen einer europaweiten Ausschreibung im Jahr 2010 zur Beschaffung einer neuen zentralen TKÜ-Systemtechnik für die Niedersächsische Polizei werden zurzeit im Bereich der Quellen-TKÜ keine aktiven Geschäftsbeziehungen zur Firma DigiTask unterhalten.

Zu 25 b:

Bei dem neuen Lieferanten für die TKÜ-Systemtechnik der Landespolizei handelt es sich um die Firma Syborg.

Zu 25 c:

Ja.

Zu 25 d:

Die Firma Syborg hat die im Vergabeverfahren geforderten Kriterien erfüllt und demzufolge den Zuschlag erhalten.

Zu 25 e:

Es wird auf die Antwort zu Frage 25 b verwiesen.

Zu 26 a:

Nein.

Zu 26 b:

Entfällt.

Zu 26 c:

Entfällt.

III. Prüfung von Qualität und Rechtmäßigkeit eingesetzter Trojaner-Software

Für die Niedersächsische Verfassungsschutzbehörde wird zur Beantwortung der Fragen 27, 28, 29 a, 30 c, 30 d, 31 b bis d, 32, 34 a bis c und 37 auf die Vorbemerkungen verwiesen.

Zu 27:

Die in den genannten Strafverfahren bei der Firma DigiTask jeweils angemietete Softwarelösung zur Durchführung der Quellen-TKÜ wurde durch die Firma DigiTask auf Grundlage der vorliegenden richterlichen Beschlüsse exakt für den konkreten Einsatz programmiert. Nach Erstellung und Übermittlung durch den Hersteller DigiTask wurde die Software im Landeskriminalamt Niedersachsen (LKA) auf einer weitestgehend dem Original entsprechenden Systemtechnik installiert und ausgiebig auf Funktionsfähigkeit und Einhaltung der richterlichen Vorgaben überprüft. Es handelte sich insoweit um eine Simulation der einzusetzenden Software vor dem Echteinsatz. Des Weiteren wurde im Rahmen der technischen und fachlichen Möglichkeiten eine Analyse der zu infiltrierenden Systemtechnik vorgenommen, um mögliche Veränderung weitestgehend auszuschließen.

Zu 28 a:

Der Quell-Code wurde vor Einsatzbeginn nicht gesichtet und ist der Landesregierung auch nicht bekannt. Die Überprüfung hinsichtlich der Recht- und Verfassungsmäßigkeit erfolgte durch umfangreiche Funktionsprüfungen des zur Verfügung gestellten Endproduktes im LKA.

Zu 28 b:

Der Quellcode einer vermarkteten Software wird als Vermögenswert eines Unternehmens beurteilt und demzufolge grundsätzlich als Geschäfts- bzw. Betriebsgeheimnis geschützt. Anstelle einer Quellcodeanalyse führte das LKA jeweils umfangreiche Anwendungstests durch.

Zu 28 c:

Entfällt.

Zu 29 a:

Überprüfungen der Software hinsichtlich der rechtlichen Vorgaben und der Funktionalität erfolgten vor Einsatzbeginn durch die Herstellerfirma DigiTask und durch das LKA.

Auf die Antworten zu den Fragen 27 und 28 wird verwiesen.

Zu 29 b:

Nein.

Zu 30 a:

Ja. Die Aktualisierungsmöglichkeit ist unerlässlich, um auf Veränderungen der Software auf dem Zielrechner reagieren zu können oder über die Möglichkeit einer vorzeitigen Beendigung bzw. Verlängerung der Überwachungsmaßnahme zu verfügen. Dass die Überwachungssoftware nicht nachträglich mit Funktionen versehen wird, die von der jeweiligen Anordnung nicht umfasst sind, wird durch technische und organisatorische Maßnahmen (Zugriffsbeschränkungen und Protokollierung am Administrationsserver und die zusätzlich zur Quellen-TKÜ erfolgende Aufzeichnung von Rohdaten am IP-Anschluss des Betroffenen) sichergestellt.

Damit wird der Vorgabe des Bundesverfassungsgerichts, nach der bei der Quellen-TKÜ auch technisch sichergestellt sein muss, dass sich die Überwachung auf laufende Telekommunikationsvorgänge beschränkt, umfassend Rechnung getragen.

Zu 30 b:

Entfällt.

Zu 30 c:

Ja.

Zu 30 d:

Die Aktualisierungsfunktion wird benötigt, um eine durchgeführte Quellen-TKÜ-Maßnahme z. B. nach richterlicher Anordnung vorzeitig beenden bzw. verlängern zu können. Des Weiteren besteht die Notwendigkeit, die eingesetzte Überwachungssoftware bei Veränderungen in der überwachten Software, dem verwendeten Betriebssystem oder anderer Softwarekomponenten auf dem Zielsystem anzupassen, um die Durchführung der Überwachungsmaßnahme durchgehend und ohne Unterbrechungen gewährleisten zu können.

Darüber hinaus gehende Funktionserweiterungen hätten speziell bei der Firma DigiTask in Auftrag gegeben werden müssen und wären dort programmiert und der Behörde kostenpflichtig zur Verfügung gestellt worden. Ein „Nachladen“ solcher speziell erstellter Funktionalitäten auf den Zielrechner wäre ausschließlich über den beim LKA installierten Administrationsserver durch das LKA selbst möglich gewesen; dabei wäre die Eingabe von zwei zusätzlichen, von der Firma DigiTask zu vergebenden Lizenzierungscodes erforderlich gewesen. Diese hätte ausschließlich das LKA vornehmen können.

Das Nachladen wäre im Aktivitäts-Logfile protokolliert worden und hätte sich auch in der Aufzeichnung der Rohdaten des IP-Anschlusses des betroffenen Rechners, die stets parallel zu einer Quellen-TKÜ erfolgt, gezeigt. Diese Vorkehrungen bieten einen wirksamen Schutz gegen ein unbemerktes Nachladen von Funktionen, die über die Überwachung laufender Telekommunikationsinhalte hinausgehen oder aus sonstigen Gründen nicht von der jeweiligen richterlichen Anordnung gedeckt sind. Der Vorgabe des Bundesverfassungsgerichts, nach der bei der Quellen-TKÜ auch technisch sichergestellt sein muss, dass sich die Überwachung auf laufende Telekommunikationsvorgänge beschränkt, wird so hinreichend Rechnung getragen.

Zu 30 e:

Entfällt.

Zu 31 a:

Der Kernbereich privater Lebensgestaltung kann durch eine Quellen-TKÜ in gleicher Weise betroffen sein wie durch sonstige Maßnahmen der Telekommunikationsüberwachung. Der Schutz dieses Kernbereiches ist in den Rechtsgrundlagen für die Telekommunikationsüberwachung ausdrücklich geregelt. Nach § 100 a Abs. 4 StPO und § 3 a G 10 darf eine Überwachung nicht durchgeführt werden, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.

Werden solche Erkenntnisse dennoch erlangt, so dürfen sie nicht verwertet werden und sind unverzüglich zu löschen. Dies gilt uneingeschränkt auch in den Fällen, in denen die Überwachung in Form der Quellen-TKÜ durchgeführt wird.

Zu 31 b:

Die Firma DigiTask hat bei Übermittlung der auf Grundlage des jeweils vorliegenden richterlichen Beschlusses angepassten Überwachungssoftware ein entsprechendes Begleitschreiben mit hinterlegtem Funktionsumfang an das LKA übersandt. Auf die Antwort zu Frage 31 a wird verwiesen.

Zu 31 c:

Bezüglich des Funktionsumfangs der eingesetzten Überwachungssoftware wurde die Zusicherung gegeben. Eingriffe in den Kernbereich privater Lebensführung sind, wie bei anderen Maßnahmen der Telekommunikationsüberwachung, nicht auszuschließen. Auf die Antwort zu Frage 31 a wird verwiesen.

Zu 31 d:

Entfällt.

Zu 32 a:

Nein. Die aufgezeigten Sicherheitslücken sind erst nach Veröffentlichung durch den CCC bekannt geworden. Die vom CCC analysierte Softwareversion wurde von niedersächsischen Behörden nicht eingesetzt.

Zu 32 b:

Die bei niedersächsischen Behörden eingesetzte Software war hinreichend gegen Eingriffe von außen geschützt. Wäre eine gezielte Manipulation der erhobenen Daten durchgeführt worden, so wäre dieser Umstand durch die simultan durchgeführte Überwachung und Aufzeichnung des IP-Anschlusses protokolliert worden und somit nachvollziehbar gewesen. Zudem hätte eine gezielte Manipulation vorausgesetzt, dass der Umstand der Überwachung, die notwendigen personenbezogenen Daten sowie die IP-Adresse bekannt gewesen wären.

Zu 32 c:

Die vom Landeskriminalamt eingesetzte Überwachungssoftware wurde vor dem Einsatz auf dem Zielsystem in einer Laborumgebung auf einer dem Zielsystem nachempfundenen Systemumgebung im LKA umfassend getestet. Hinweise auf eine größere Anfälligkeit für weitere Angriffe von außen haben sich nicht ergeben.

Zu 32 d:

Durch den Einsatz der Überwachungssoftware sind bei den infiltrierten Rechnern keine Funktionsbeeinträchtigungen bekannt oder festgestellt worden. Darüber hinausgehende Informationen liegen der Landesregierung nicht vor.

Zu 33:

Eingriffe in die Rechte der Kommunikationspartner des überwachten Anschlusses sind bei jeder Form der Telekommunikationsüberwachung unvermeidlich und von den entsprechenden Rechtsgrundlagen gedeckt. Insoweit besteht kein Unterschied zur Überwachung der Telekommunikation ohne Überwachungssoftware. Kommunikation (per Telefon, E-Mail, Skype etc.) findet regelmäßig zwischen zwei oder mehr Teilnehmern statt. Von der Überwachung der Zielperson sind daher zwangsläufig stets auch deren Kommunikationspartner betroffen.

Zu 34 a:

Die Landespolizei hat in der Vergangenheit keine „multifunktionalen Rohlinge“ erworben. Die bezogene Überwachungssoftware wurde in jedem Einzelfall auf Grundlage der ergangenen richterlichen Beschlüsse für den konkreten Einzelfall nach Auftragserteilung durch das LKA durch die Firma DigiTask programmiert. Als Auftragnehmer war die Firma DigiTask für die fehlerfreie Programmierung der Software zuständig. Die gelieferte Software wurde in jedem Einzelfall vor dem Einsatz in einer simulierten Testumgebung durch das LKA ausgiebig hinsichtlich der gelieferten Funktionalitäten getestet.

Für die mit der neuen TKÜ-Systemtechnik der Firma Syborg beschaffte Software kann das LKA die im konkreten Einzelfall erforderliche Konfiguration der Software selbst vornehmen.

Zu 34 b:

Auf die Ausführungen zu Frage 34 a und Frage 8 wird verwiesen.

Zu 34 c:

Nach Programmierung und Übermittlung der Überwachungssoftware durch den Hersteller DigiTask wurde die Software auf einer weitestgehend dem Original entsprechenden Systemtechnik installiert und ausgiebig auf Funktionsfähigkeit und Einhaltung der geforderten richterlichen Vorgaben überprüft. Es handelt sich insoweit um eine Simulation der einzusetzenden Software vor dem Echteinsatz.

Auf die Ausführungen zu Frage 27 und die Vorbemerkungen wird verwiesen.

Zu 34 d:

Der Landesbeauftragte für den Datenschutz wurde bei den bisher durchgeführten Maßnahmen der Quellen-TKÜ nicht beteiligt. Eine Beteiligung ist rechtlich nicht vorgesehen. In die Beschaffung der neuen zentralen TKÜ-Systemtechnik ist er jedoch eingebunden.

Für weitere Ausführungen wird auf die Antwort zu Frage 42 a verwiesen.

Zu 35:

Die Software war in der eingesetzten Form ausschließlich zur Durchführung der Quellen-TKÜ geeignet.

Auf die Vorbemerkungen sowie die Antworten zu den Fragen Nummer 3 und 30 wird verwiesen.

Zu 36 a:

Steuerungsbefehle im Sinn einer Aktualisierungsfunktion können ausschließlich durch die jeweilige Sicherheitsbehörde und nur über den dort vorhandenen Administrationsserver an das Zielsystem übermittelt werden. Hierauf hat die Herstellerfirma keinen Zugriff. Auf die Antwort zu Frage 30 d wird verwiesen.

Zu 36 b:

Der Zugriff nicht autorisierter Personen auf das Zielsystem ist allenfalls eine theoretische Möglichkeit; Unbefugte müssten über IP-Adresse, Übertragungsprotokoll, Kenntnis des Verschlüsselungsverfahrens und Schlüssel verfügen.

Unbefugten Dritten und damit auch der Firma DigiTask waren weder die IP-Adresse des überwachten Endgerätes bekannt noch der Zugriff auf den Administrationsserver im LKA möglich. Dieser befindet sich in speziell gesicherten Räumlichkeiten des LKA, deren Zugang nur für einen eingeschränkten gesondert berechtigten Personenkreis zugänglich ist. Des Weiteren wäre jeder rechtswidrige Zugriff auf das überwachte Endgerät durch die simultan durchgeführte IP-Anschlussüberwachung registriert und protokolliert worden. Derartige Zugriffe oder Zugriffsversuche hat es nicht gegeben.

Zu 37:

Die Nachladefunktion mit der Zielrichtung, zusätzliche Funktionalitäten auf das Zielsystem aufzuspielen, wurde nicht genutzt und wäre auch nur möglich gewesen, wenn die Firma DigiTask erneute Aufträge zur erweiterten Programmierung der Software erhalten hätte. Auf die Antworten zu den Fragen 30 und 35 wird verwiesen.

Die Nachladefunktion ist mit der Zielrichtung einer Aktualisierung in der Art genutzt worden, dass in beiden durchgeführten Strafverfahren der Polizei die Überwachung des Endgerätes vor Ablauf des ursprünglichen Beschlusses beendet wurde.

IV. Datenschutz und Datensicherheit

Für die Niedersächsische Verfassungsschutzbehörde wird zur Beantwortung der Fragen 38, 39 und 41 auf die Vorbemerkungen verwiesen.

Zu 38 a:

Zur Verschleierung des Kommunikationsverkehrs wurden die bei den Überwachungsmaßnahmen der Landespolizei und des Zolls 2009 und 2011ausgeleiteten Daten auf dem überwachten Endgerät verschlüsselt über einen amerikanischen Server an den Aufzeichnungsserver in Deutschland weitergeleitet. Eine Speicherung der ausgeleiteten Daten auf diesen Servern erfolgte nicht. Es handelte sich lediglich um die Weiterleitung eines verschlüsselten Datenstroms. Die Verschleierung erfolgte aus taktischen Gründen.

Zu 38 b:

Der Server wurde bei dem Hostingprovider WebIntellects angemietet.

Zu 39 a:

Bei den in den Jahren 2009 und 2011 durchgeführten Überwachungsmaßnahmen wurden die erhobenen Daten auf dem überwachten Endgerät verschlüsselt über einen amerikanischen Server an den Aufzeichnungsserver in Deutschland ausgeleitet. Auf dem amerikanischen Server wurden die Daten nicht gespeichert, sondern lediglich zur Verschleierung des Kommunikationsverkehrs durchgeleitet.

Es wurden ausschließlich verschlüsselte Datensätze übertragen, die im Klartext nicht lesbar waren.

Zu 39 b:

Die verschlüsselte Durchleitung von Daten stellt nach Auffassung des Datenschutzbeautragten des BKA keine Datenübermittlung i. S. datenschutzrechtlicher Vorschriften dar. Insoweit ist § 4 b BDSG bei einer Datendurchleitung nicht einschlägig.

Auf die Antwort zu Frage 39 a wird verwiesen.

Zu 40 a:

Das LKA Niedersachsen hatte mit dem in Luxemburg ansässigen Kommunikationsdienstleister Skype allgemein und im Vorfeld der Überwachungsmaßnahmen Gespräche geführt, um eventuell bestehende Möglichkeiten einer Gesprächsausleitung zu erörtern. Dabei ist zu berücksichtigen, dass ausländische Anbieter nach dem Telekommunikationsgesetz nicht zur Ausleitung verpflichtet werden können.

Zu 40 b:

Entfällt.

Zu 40 c:

Nach offizieller Aussage der Firma Skype gegenüber dem LKA ist es nicht möglich, die im Skype-Netzwerk geführte Kommunikation unverschlüsselt auszuleiten. Die zwischen zwei Skype-Clients geführte Kommunikation wird auf skype-fremden Netzwerken geführt und baut auf einer 256-Bit-AES-Verschlüsselung auf. Die eingesetzten Verschlüsselungscodes werden unter Zuhilfenahme des RSA-Verfahrens (1536 bis 2048 Bit) übermittelt. Die zur Entschlüsselung der übermittelten Daten benötigten privaten Entschlüsselungscodes liegen dabei nur an den Endpunkten, also bei den Kommunikationspartnern, temporär vor. Daraus folgt, dass der Dienstleister die entsprechende Kommunikation nur verschlüsselt hätte zur Verfügung stellen können. Eine Entschlüsselung der Kommunikation ist auch der Firma Skype nicht möglich.

Zu 40 d:

Entfällt.

Zu 41 a:

Mittels Überwachungssoftware wurde in Niedersachsen durch die Polizeibehörden keine E-Mail-Kommunikation überwacht.

Zu 41 b:

Die angesprochenen Kommunikationsdienste wurden bisher nicht überwacht.

Zu 41 c:

Entfällt.

Zu 41 d:

Entfällt.

Zu 42 a:

Zunächst wird auf die Antwort zu Frage 34 d verwiesen.

Die Aussage in der TV-Sendung „PhoenixRunde“ am 13.10.2011 bezog sich auf die Beteiligung des Landesbeauftragten für Datenschutz (LfD) im Rahmen der Beschaffung der neuen zentralen TKÜ-Systemtechnik der Landespolizei. Im Zuge dieser Beschaffungsmaßnahme wurden dem LfD in einem vom LKA durchgeführten Gespräch am 23.09.2010 die Möglichkeiten der neuen TKÜ-Systemtechnik erläutert. Durch diesen Informationsaustausch wurde der LfD frühzeitig in die Thematik eingebunden und gebeten, eventuell vorliegende datenschutzrechtliche Bedenken frühzeitig mitzuteilen.

Die Überwachungssoftware zur Durchführung der Quellen-TKÜ, die zu der neuen Systemtechnik gehört, wurde dem LfD am 16.12.2011 im Rahmen einer Präsentation im Ministerium für Inneres und Sport vorgestellt. Dabei wurde mit Blick auf einen bundesweit vereinbarten Qualitätssicherungsprozess der künftigen Überwachungssoftware durch das im Bundeskriminalamt im Aufbau befindliche Kompetenzzentrum Informationstechnische Überwachung und ein dazu vorgesehenes externes Expertengremium deutlich die Vorläufigkeit des Produkts herausgestellt. Der LfD in Niedersachsen wird bis zur endgültigen Freigabe der Überwachungssoftware am weiteren Entwicklungsprozess beteiligt

Für eine Einbindung des LfD in die Durchführung von Ermittlungsmaßnahmen in laufenden Strafverfahren gibt es auch keine Rechtsgrundlage; eine solche Beteiligung wäre außerdem systemfremd.

Für den Bereich des Verfassungsschutzes erfolgt im Vorfeld von G 10-Maßnahmen grundsätzlich keine Einbeziehung des LfD. Der LfD besitzt für diesen Bereich keine Kontrollbefugnis. Es kommen das G 10 und das Niedersächsische Gesetz zur Ausführung des Artikel 10-Gesetzes (Nds. AG 10) als lex specialis gegenüber dem Niedersächsischen Datenschutzgesetz zur Anwendung.

§ 15 Abs. 5 Satz 1 G 10 und § 4 Abs. 1 Nds. AG G 10 sehen eine Zuständigkeit der G 10-Kommission hinsichtlich der Entscheidung über die Notwendigkeit und Zulässigkeit von G 10-Maßnahmen vor. Die Kontrolle der Kommission erstreckt sich nach § 15 Abs. 5 Satz 2 G 10 und § 4 Abs. 2 Nds. AG G 10 auch auf die Verarbeitung der nach dem G 10 erhobenen personenbezogenen Daten.

Nach diesen gesetzlichen Vorschriften darf dem LfD keine Auskunft über die Durchführung von G 10-Maßnahmen, einschließlich Quellen-TKÜ-Maßnahmen, erteilt werden, sofern nicht ausnahmsweise die G 10-Kommission den LfD nach § 4 Abs. 3 Nds. AG G 10 ersucht, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

Zu 42 b:

Eine abschließende Bewertung durch den Landesdatenschutzbeauftragten liegt noch nicht vor.

Zu 42 c:

Entfällt.

Zu 43 a:

Es handelt sich hierbei nicht um ein spezielles Problem der (Quellen-)Telekommunikationsüberwachung. Bei jeder Ermittlungsmaßnahme, unabhängig davon, ob diese verdeckt oder offen durchgeführt wird, besteht die Möglichkeit, dass die Ermittlungspersonen Dinge erfahren, die aus Sicht des Betroffenen geheim bleiben sollen.

Lediglich ergänzend wird auf Folgendes verwiesen: Da die eingesetzte Software ausschließlich zur Überwachung von über das Internet geführten Telefonaten genutzt werden konnte, hätten die Strafverfolgungsbehörden nur dann Kenntnis von Daten, „zu deren Geheimhaltung sich die überwachte Person verpflichtet hat (z. B. PIN für Onlinebanking oder vertrauliche Geschäftsdaten)“ bekommen können, wenn die Person diese Daten gegenüber ihrem Gesprächspartner offenbart hätte.

Zu 43 b:

Es handelt sich nicht um ein spezielles Problem der (Quellen)-Telekommunikationsüberwachung. Die Kenntniserlangung durch die Ermittlungsbehörden ist durch die jeweilige Eingriffsnorm gedeckt.

Zu 44 a:

Die Benachrichtigung über verdeckte Ermittlungsmaßnahmen richtet sich nach den Voraussetzungen des § 101 StPO, bei gemäß § 100 a StPO durchgeführten Telekommunikationsüberwachungsmaßnahmen speziell nach § 101 Abs. 4 Nr. 3 StPO.

In den genannten staatsanwaltlichen Verfahren wurden die Beschuldigten über die durchgeführten Maßnahmen benachrichtigt. Weitergehende Benachrichtigungen (unbeteiligte Kommunikationspartner) wurden und werden fortlaufend entsprechend den Vorgaben des § 101 StPO geprüft und durchgeführt.

Im Bereich des Verfassungsschutzes gilt für die Quellen-TKÜ, ebenso wie für die herkömmliche TKÜ, die Benachrichtigungspflicht nach § 12 G 10 i. V. m. § 4 Abs. 5 und 6 Niedersächsisches Gesetz zur Ausführung des Artikel 10-Gesetzes. Ansonsten wird auf die Antwort zu Frage 1 verwiesen.

Zu 44 b:

Es hat keine erfolglosen Versuche gegeben. Auf die Antwort zu Frage 8 wird verwiesen.

Zu 44 c:

Der Landesbeauftragte für Datenschutz wurde nicht über geplante, erfolgende und erfolgte Einsätze von Überwachungssoftware im Bereich der Landespolizei informiert, da eine entsprechende rechtliche Verpflichtung nicht besteht.

Für die Niedersächsische Verfassungsschutzbehörde wird auf die Beantwortung zu Frage 42 verwiesen.

V. Gerichtliche Verwertbarkeit der ermittelten Daten

Zu 45:

Der Landesregierung sind bundesweit keine Entscheidungen bekannt, bei denen ein Gericht ein Beweisverwertungsverbot im Hinblick auf Kommunikationsinhalte angenommen hätte, die mittels Quellen-TKÜ erlangt wurden. Der Vorwurf der Manipulation lässt sich zudem durch eine sorgfältige Dokumentation entkräften.

Um eine Dokumentation sicherzustellen, werden alle an den Aufzeichnungsserver übermittelten Kommunikationsdaten anhand von Log-Files entsprechend protokolliert. Bei der automatisierten Protokollierung wird u. a. die IP-Adresse von der übermittelnden Gegenstelle aufgezeichnet. Neben der Quellen-TKÜ erfolgt simultan auch eine IP-Anschlussüberwachung bei der betroffenen Zielperson. Somit steht die zum Zeitpunkt der Datenübertragung genutzte IP-Adresse fest und kann mit der zur Datenübertragung auf den Aufzeichnungsserver übermittelten IP-Adresse bei Bedarf abgeglichen werden.

Zur Manipulation der Überwachungsmaßnahme wäre es insgesamt erforderlich gewesen, dass die Überwachung des Endgerätes, der Authentifizierungscode zur Anmeldung am Aufzeichnungsserver, die zur Datenübertragung genutzte Verschlüsselung samt Verschlüsselungscode und die Möglichkeit der Datenübertragung mit den vorgenannten Parametern bekannt gewesen wären. Des Weiteren hätte die Datenübermittlung zum Aufzeichnungsserver direkt vom überwachten IP-Anschluss der Zielperson erfolgen müssen.

In den niedersächsischen Ermittlungsverfahren, in denen eine Quellen-TKÜ durchgeführt wurde, ist die Verwertbarkeit der damit gewonnenen Daten nicht problematisiert worden. Während im Verfahren der Staatsanwaltschaft Hannover wegen des Handeltreibens mit Betäubungsmitteln in nicht geringer Menge der Angeklagte rechtskräftig zu einer Freiheitsstrafe von zwei Jahren und neun Monaten verurteilt wurde, dauern die anderen Verfahren noch an.

Auf die Ausführungen zu den Fragen 32 b und c wird hingewiesen.

Zu 46 a:

Es handelt sich um eine Frage, die auch in anderen Ermittlungseingriffen immanent ist. So wird beispielsweise von des Drogenhandels verdächtigen Personen nicht nur vereinzelt behauptet, die aufgefundenen Betäubungsmittel seien im Rahmen einer Durchsuchung durch Polizeibeamte untergeschoben worden. Dieser Einlassung kann u. a. durch sorgfältige Dokumentation der Eingriffshandlung begegnet werden.

Ziel einer forensischen Analyse ist es, zu ermitteln, welche Daten sich auf einer zu überprüfenden Festplatte befinden und woher diese stammen. Grundsätzlich lässt sich in keinem Verfahren ausschließen, dass Daten durch unbefugte Dritte auf das entsprechende Zielsystem aufgespielt wurden. Diese Feststellungen zu treffen, ist Gegenstand der forensischen Analyse.

In den polizeilichen geführten Ermittlungsverfahren mit durchgeführten Quellen-TKÜ-Maßnahmen wird gesondert protokolliert, dass es zum Einsatz einer Überwachungssoftware gekommen ist. Sollten unberechtigte Datenübertragungen im Rahmen des Einsatzes der Überwachungssoftware erfolgt sein, so ist dieses durch die simultan durchgeführte IP-Anschlussüberwachung beweissicher aufgezeichnet.

Die Verfassungsschutzbehörde verfügt nicht über Exekutivbefugnisse, sodass sich die Beantwortung auf Maßnahmen der Ermittlungsbehörden bezieht.

Zu 46 b:

Auf die Antwort zu Frage 7 wird verwiesen.

Zu 46 c:

Das Aufspielen der Software auf den zu infiltrierenden Rechner erfolgt durch die Ermittlungsbehörden nach dem Vier-Augen-Prinzip. Das heißt: zwei Mitarbeiter sind zeitgleich für die Implementierung der Software und die Rechtmäßigkeit der Maßnahme verantwortlich.

Teil der forensischen Analyse ist der Nachweis, woher die auf einer sichergestellten Festplatte festgestellten Daten stammen. Die Behauptung, die Ermittlungsbehören hätten belastendes Material auf den Computer im Rahmen der Überwachungsmaßnahmen geladen, lässt sich durch die automatisierte und zeitgleich mit der Quellen-TKÜ durchgeführte Überwachung des IP-Anschlusses überprüfen. Zudem ist dieses Vorgehen seitens der Beschuldigten nicht auf den Bereich der Quellen-TKÜ begrenzt, sondern ein im Bereich der Beweisführung häufiger auftretendes Problem.

VI. Grundsätzliche Verfassungsmäßigkeit von Trojaner-Software

Zu 47:

Nach § 3 Nr. 22 Telekommunikationsgesetz (TKG) ist Telekommunikation der „technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“ und umfasst alle damit verbundenen Vorgänge, d. h. die eigentliche Kommunikation mit ihren Inhalten sowie auch die zur Herstellung der Verbindung notwendigen Handlungen bzw. Vorgänge bis zu deren Beendigung (s. auch Bär, TK-Überwachung, Kommentierung zu §§ 100 a bis 101 StPO, § 100 a StPO Rz. 10 und 57).

§ 100 a StPO, der die Überwachung der Telekommunikation bei Vorliegen des Verdachts einer schweren Straftat nach § 100 a Abs. 2 StPO regelt, sowie die §§ 1 und 3 G 10, die den Verfassungsschutzbehörden unter bestimmten Voraussetzungen die Überwachung der Telekommunikation gestatten, beschränken die Überwachungsmaßnahme nicht auf bestimmte Bereiche des Telefonierens, sondern erfassen generell die gesamte Telekommunikation. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 27. Februar 2008 zur im nordrhein-westfälischen Verfassungsschutzgesetz geregelten Online-Durchsuchung ausgeführt, dass bei einer Quellen-TKÜ ausschließlich ein Eingriff in Artikel 10 GG (Fernmeldegeheimnis) vorliegt, der über § 100a StPO bzw. die §§ 1 und 3 G 10 gerechtfertigt wäre. In der Entscheidung des BVerfG heißt es zur Quellen-TKÜ u. a.:

„Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff allein an Artikel 10 Abs. 1 GG zu messen.

Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt (vgl. BVerfGE 106, 28 <37 f.>; 115, 166 <186 f.>).

Artikel 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung', wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein" (RN 190).

Bei den in Niedersachsen durchgeführten Maßnahmen der Quellen-TKÜ waren diese Vorgaben erfüllt. Zum einen enthielten die richterlichen Anordnungen sämtlich die Beschränkung, nur Internettelefonie auszuleiten. Zum anderen ist durch das LKA sichergestellt worden, dass nur entsprechende Technik eingesetzt wurde.

Auf die Antworten zu Frage 27 und Frage 28 wird verwiesen.

Uwe Schünemann

(Ausgegeben am 08.03.2012
Unkorrigierter Vorabdruck ausgegeben am 09.03.2012)