Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion DIE LINKE.

Grenzüberschreitendes behördliches Ausspähen fremder Rechnersysteme ("Governmental Hacking")

BT-Drucksache 17/5369

---

1. Welche Initiativen wurden auf EU-Ebene seit 2007 in strafprozessualer sowie juristischer Hinsicht ergriffen, um „Maßnahmen zur Erleichterung von Ferndurchsuchungen" voranzutreiben?

Zu 1.
Der Bundesregierung sind keine solchen Maßnahmen bekannt.

2. Welche legislativen oder operativen Maßnahmen wurden für die Zukunft vorgeschlagen oder anvisiert und welche Haltung hat die Bundesregierung hierzu eingenommen?

Zu 2.
Auf die Antwort zu Frage 1 wird verwiesen.

3. Inwiefern werden Überlegungen zur „Erleichterung von Ferndurchsuchungen" in die Diskussionen um die Ausgestaltung der „Europäischen Ermittlungsanordnung in Strafsachen" bzw. des „Rahmenbeschlusses über die Europäische Beweisanordnung" eingebracht?

Zu 3.
Der Anwendungsbereich der Europäischen Beweisanordnung (EBA) erfasst die Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafsachen. Die EBA soll durch den Richtlinienvorschlag über die Europäische Ermittlungsanordnung in Strafsachen (EEA) ersetzt werden. Damit soll die bisherige Parallelität von Rechtsinstrumenten der tradierten Rechtshilfe und von Rechtsinstrumenten der gegenseitigen Anerkennung im Bereich der grenzüberschreitenden Beweiserhebung künftig möglichst vermieden werden. Sogenannte "Ferndurchsuchungen" wurden bisher von keiner Seite in die Verhandlungen eingebracht.
Die Bundesregierung führt die Verhandlungen zur EEA in dem Verständnis, dass die Anerkennung und Vollstreckung von Ermittlungsmaßnahmen, um die andere Mitgliedstaaten der Europäischen Union Deutschland mit einer EEA ersuchen, nur in Betracht kommt, wenn die Durchführung der Maßnahme nach deutschem Recht zulässig wäre.

Die Bundesregierung setzt sich seit Beginn der Verhandlungen dafür ein, hierzu im Richtlinientext ausreichend klare Regelungen zu treffen.
Für den Erlass von EEAs wurde von der zuständigen Ratsarbeitsgruppe - auch auf Betreiben der Bundesregierung - in Ergänzung des ursprünglichen Richtlinienvorschlags bereits eine Regelung erarbeitet, die besagt, dass eine EEA nur in Betracht kommt, wenn die in der EEA benannte Ermittlungsmaßnahme bei einem vergleichbaren innerstaatlichen Fall erlassen werden könnte. Damit ist sichergestellt, dass Strafverfolgungsbehörden nicht mittels einer EEA um Strafverfolgungsmaßnahmen im Ausland ersuchen, die innerstaatlich nicht zulässig wären.

4. Welche Arbeitsgruppen existieren bei welchen EU-Agenturen bzw. EU-Institutionen (auch SitCen und ESVP) zur Entwicklung von „Ferndurchsuchungen" oder ähnlicher Initiativen und wie sind deutsche Behörden daran beteiligt?

Zu 4.
Der Bundesregierung sind keine Arbeitsgruppen im Sinne der Fragestellung bekannt.

5. Welche Rolle spielt die „Cross-Border Surveillance Working Group" bezüglich der Entwicklung von „Maßnahmen zur Erleichterung von Ferndurchsuchungen" oder ähnlicher Initiativen?

Zu 5.
Die Entwicklung von „Maßnahmen zur Erleichterung von Ferndurchsuchungen" ist nicht Gegenstand der Cross-Border-Surveillance Working Group.

6. Wie oft hat sich die „Cross-Border Surveillance Working Group" in den letzen fünf Jahren getroffen und welche konkrete Inhalte wurden behandelt (bitte nach Tagesordnung der jeweiligen Treffen aufschlüsseln)?

Zu 6.
Es finden jährlich zwei Treffen der Cross-Border-Surveillance Working Group (CSW) statt, in denen in einem Erfahrungsaustausch Fachvorträge zur grenzüberschreitenden Observation und damit zusammenhängenden Problemstellungen mit dem Ziel der Optimierung von Arbeitsabläufen gehalten werden.

Bei den Treffen der CSW findet regelmäßig eine Vorstellung der Dienststellen und der spezifischen Arbeitsweise der teilnehmenden Länder statt; in diesem Zusammenhang werden neben den operativen und taktischen Möglichkeiten auch die rechtlichen Rahmenbedingungen dargestellt. Präsentationen informieren die Teilnehmer über den Einsatz von Angehörigen mobiler Observationskräfte; so wurde unter anderem durch den Staatsschutz des BKA ausführlich über den „Sauerland-Fall" berichtet. Vertreter teil-

nehmender Ländern haben vergleichbare Einsätze zu Verfahren auch aus anderen Deliktsbereichen der organisierten und allgemeinen Kriminalität geschildert. Auf den Tagesordnungen der CSW steht zudem die organisatorische Ausgestaltung der Arbeitsgruppe.

7. Hat Europol nach Kenntnis der Bundesregierung jemals versucht, sowohl die Kommunikation fremder Rechnersysteme oder auf den Geräten befindliche Inhalte oder Passwörter durch den Einsatz von Software zu auszuspähen? Welche Einzelheiten sind der Bundesregierung hierzu bekannt?

Zu 7.
Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

8. Haben Behörden anderer Regierungen (innerhalb und außerhalb der EU) nach Kenntnis der Bundesregierung jemals versucht, sowohl die Kommunikation von Rechnersystemen in Deutschland oder auf den Geräten befindliche Inhalte oder Passwörter durch den Einsatz von Software zu auszuspähen? Welche Einzelheiten sind der Bundesregierung hierzu bekannt?

Zu 8.
Angriffe auf die Vertraulichkeit von Rechnersystemen mittels Schadprogrammen finden nach Erkenntnissen der Bundesregierung häufig statt. Hiervon sind Unternehmen, Forschungseinrichtungen, Behörden und Privatpersonen gleichermaßen betroffen. Nach Erkenntnissen des Bundesamtes für Sicherheit in der Informationstechnik werden durchschnittlich fünf gezielte Angriffe täglich auf Personen als Nutzer des Regierungsnetzes detektiert und abgewehrt. Ob es sich bei den Urhebern dieser Angriffe um öffentliche Stellen handelt oder ob ein krimineller Hintergrund vorliegt, ist nicht bekannt. Gleichwohl ist eine nachrichtendienstliche Steuerung oder zumindest Beteiligung staatlicher Stellen angesichts der ausgewählten Ziele und der angewandten Methoden in vielen Fällen wahrscheinlich.

9. Hat der ATK inzwischen eine „nähere Erläuterung" seiner „Empfehlungen" vom September 2010 vorgelegt und welchen Inhalt hatte diese bezüglich der Entwicklung von „Maßnahmen zur Erleichterung von Ferndurchsuchungen"? Falls nein, wann ist mit der Erläuterung zu rechnen?

Zu 9.
Die Handlungsempfehlung 3 des EU-Anti-Terrorismusbeauftragten erwähnt neben einer verbesserten gegenseitigen Kenntnis bewährter Praktiken und der Erstellung von Mustervereinbarungen auch die Festlegung eines gemeinsamen justiziellen Rahmens für bestimmte Ermittlungstechniken wie z.B. den Einsatz von verdeckten Ermittlern oder Informanten oder Online-Durchsuchungen, sowie die Präzisierung der bei grenzüber-

greifenden Überwachungen zu beachtenden Regeln. Dem Wortlaut der Empfehlung kann nach Ansicht der Bundesregierung nicht entnommen werden, dass damit "Maßnahmen zur Erleichterung von Ferndurchsuchungen" (so die Formulierung in Frage Nr. 9) oder Forderungen nach "Änderung der Rechtsordnung bezüglich des behördlichen Eindringens in fremde Rechnersysteme" (so die Formulierung in Frage Nr. 10) gefordert werden.

Für eine inhaltliche Bewertung der Handlungsempfehlung 3 durch die Bundesregierung bedürfte es weiterer Erläuterungen des EU-Anti-Terrorismusbeauftragten zu seinen konkreten Vorstellungen. Ob allerdings, bzw. wann eine Konkretisierung seiner Vorstellungen stattfindet, hat der EU-Anti-Terrorismusbeauftragte bislang nicht mitgeteilt.

Nach der Vorstellung der Handlungsempfehlungen des EU-Anti-Terrorismusbeauftragten im September 2010 wurde in den zuständigen Ratsgremien mittlerweile Einigkeit über ein „Follow-up-Papier" der ungarischen Ratspräsidentschaft (Ratsdokument 5764/1/11 vom 31. März 2011) erzielt. Das „Follow-up-Papier" verzichtet bewusst auf eine inhaltliche Bewertung der Handlungsempfehlungen und legt nur das Verfahren für die weitere Prüfung der Empfehlungen fest. Es avisiert also keine Gesetzgebungsinitiative zu "Online-Durchsuchungen".

Für die ergebnisoffene Prüfung der Handlungsempfehlung 3 sind der Ständige Ausschuss des Rates für innere Sicherheit (COSI), die Ratsarbeitsgruppe für die Zusammenarbeit in Strafsachen (COPEN) und die Arbeitsgruppe für allgemeine Angelegenheiten, einschließlich Evaluierungen (GENVAL) vorgesehen.

10. Wie bewertet die Bundesregierung die vom ATK aufgeworfenen Forderungen nach Änderungen der Rechtsordnung bezüglich des behördlichen Eindringens in fremde Rechnersysteme?

Zu 10.
Auf die Antwort zu Frage 9 wird verwiesen.

11. Wie bewertet die Bundesregierung das „Follow-up" des Brainstormings des ATK (Ratsdokument 5764/11), das unter anderem eine Gesetzgebungsinitiative zu „Onlinedurchsuchungen" anvisiert?

Zu 11.
Auf die Antwort zu Frage 9 wird verwiesen.

12. Welche Haltung nimmt die Bundesregierung in den Diskussionen zum Ratsdokument 5764/11 ein?

Zu 12.
Auf die Antwort zu Frage 9 wird verwiesen.

13. Welchen Mehrwert verspricht sich die Bundesregierung hinsichtlich von „Maßnahmen zur Erleichterung von Ferndurchsuchungen" durch den im Ratsdokument 5957/2/10 REV 2 anvisierten Einbezug von „EMSI, CEPOL, Eurojust, Europol, ENISA" sowie „Interpol, VN" und welche Institutionen sind mit „usw." gemeint?

Zu 13.
Das Ratsdokument 5957/2/10 REV 2 enthält einen Entwurf von Schlussfolgerungen des Rates zu einem Aktionsplan für die Umsetzung der konzertierten Strategie zur Bekämpfung der Cyberkriminalität in allgemeiner Form. Ein spezifischer Bezug zu den in der Frage angesprochenen „Ferndurchsuchungen" besteht nicht. Die Förderung der Zusammenarbeit zwischen europäischen und internationalen Stellen bezüglich neuer Technologien wird zu einem Wissenstransfer führen, der es den betroffenen Einrichtungen erleichtern soll, ihre Aufgabe effektiver zu erfüllen, um damit einen Beitrag zur erfolgreichen Bekämpfung der Internetkriminalität zu leisten. Neben den genannten Einrichtungen sind alle Stellen gemeint, die über verwertbares Wissen im Bereich der Bekämpfung der Internetkriminalität verfügen.

14. Was ist damit gemeint, wenn eine „Partnerschaft zwischen der Polizei und dem privaten Sektor" befördert werden soll, die im Ratsdokument 15569/08 vom Kommissionspräsident aufgefordert werden „auf das Mittel der Ferndurchsuchung zurückzugreifen"?

Zu 14.
Eine entsprechende Aufforderung ist in dem Dokument nicht enthalten.

15. Welche Initiativen wurden bezüglich dieser „Partnerschaft zwischen der Polizei und dem privaten Sektor" bislang ergriffen?

Zu 15.
Auf die Antwort zu Frage 14 wird verwiesen.

16. Welchen Inhalt hat die Tagung „Forensic Science relating to Counter Terrorism", die vom 14.-17. Juni in Polen stattfindet, bezüglich der Weiterentwicklung des behördlichen grenzüberschreitenden Ausspähens fremder Rechnersysteme?

Zu 16.
Über den Inhalt der Tagung liegen der Bundesregierung keine Erkenntnisse vor.

17. Welche Voraussetzungen bzw. rechtlichen Rahmenbedingungen müssen erfüllt sein, damit deutsche Behörden ihre Zustimmung zu „Ferndurchsuchungen" von in Deutschland befindlichen Rechnern durch Polizeien anderer Regierungen geben?

Zu 17.
Bei eingehenden Ersuchen um strafrechtliche Zusammenarbeit wird die hoheitliche Maßnahme in Deutschland auf der Grundlage des nationalen Rechts von Angehörigen deutscher Dienststellen ausgeführt. Dies gilt auch, soweit der Richtlinienentwurf zur Europäischen Ermittlungsanordnung (EEA) die Möglichkeit vorschlägt, dass Vertreter des Anordnungsstaats bei der Durchführung der in der EEA benannten Ermittlungsmaßnahme im Vollstreckungsstaat zugegen und unterstützend tätig sein können. Denn eine Verpflichtung für den Vollstreckungsstaats, Vertretern des Anordnungsstaats die Ausübung hoheitlicher Maßnahmen zu gestatten, ist in der EEA nicht vorgesehen.

18. Wie ist der Stand der technischen Entwicklung von Fähigkeiten des BKA, „entfernte PC auf verfahrensrelevante Inhalte hin untersuchen zu können, ohne tatsächlich am Standort des Gerätes anwesend zu sein", wie es der früherer Innenminister Wolfgang Schäuble gemäß der Drucksache 16/3231 in einer Unterlage für den Haushaltsausschuss des Deutschen Bundestages unter der Überschrift „Online-Durchsuchung" ausführt (bitte hinsichtlich etwaiger verschiedener Projekte erläutern)?

Zu 18.
Das Bundeskriminalamt ist gemäß §§ 4a, 20k BKAG befugt, unter den dort genannten Voraussetzungen im Einzelfall einen verdeckten Eingriff in informationstechnische Systeme vorzunehmen. Das Bundeskriminalamt hat die für einen solchen Eingriff erforderlichen und den rechtlichen Voraussetzungen genügenden Einsatzmittel (sog. Remote Forensic Software) entwickelt.

19. Welches „hierfür notwendige Instrumentarium" ist seitdem, wie vom zwischenzeitlich entlassenen früheren Staatssekretär August Hanning ausgeführt, entwickelt worden?

Zu 19.
Auf die Antwort zu Frage 18 wird verwiesen.

20. Welche Bundes- und Landesbehörden von Polizei und Verfassungsschutz führen nach Kenntnis der Bundesregierung bereits sogenannte „Onlinedurchsuchungen" durch, wie es etwa dem Verfassungsschutz Nordrhein-Westfalens seit 2006 als „heimliche[r] Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel" gestattet ist?

Zu 20.
Auf Bundesebene hat nur das Bundeskriminalamt nach § 20 k BKAG die Befugnis, zur Gefahrenabwehr "Onlinedurchsuchungen" durchzuführen, und macht davon Gebrauch. Soweit sich die Frage auch auf die Praxis der Landesbehörden bezieht, weist die Bundesregierung darauf hin, dass sich der parlamentarische Informationsanspruch nicht auf Gegenstände erstreckt, die keinen Bezug zum Verantwortungsbereich der Regierung gegenüber dem Bundestag haben, insbesondere weil sie sich außerhalb der Zuständigkeit der Bundesregierung befinden (BVerfGE 124, 161 [188, 196]). Dem entsprechend hat die Bundesregierung keine detaillierte Kenntnis über zurzeit stattfindende Maßnahmen von Landesbehörden, da sie von Seiten der Länder darüber nicht in strukturierter Form informiert wird.

21. Inwieweit hat die Bundesregierung Forschungs- und Entwicklungsprojekte gefördert oder betrieben, bei denen als „Computerschadprogramme" zu qualifizierende Software, z.B. zur Entwicklung und Tests von Abwehrkonzepten, entwickelt oder eingesetzt werden?

Zu 21.
Im Rahmen der Untersuchung von Handy-Sicherheit ist seitens der Universität München ein hardwarebasierter Angriff entwickelt und auf dem BSI-Kongress im Jahre 2009 vorgestellt worden. Ziel war es, auf Schwachstellen bei der Sicherheit von Mobilfunkgeräten hinzuweisen.

22. Wie bewertet die Bundesregierung die Forderungen der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder nach Prüfung der Zulässigkeit der Voraussetzungen der Quellen-Telekommunikationsüberwachung „unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts"?

Zu 22.
Die Bundesregierung respektiert die Vorgaben des Bundesverfassungsgerichts.

23. Wie bewertet die Bundesregierung die Einschätzung der Datenschutzbeauftragten, dass polizeiliche und geheimdienstliche Spähsoftware zum Abhören von Kommunikation „in der Vorgehensweise einer Online-Durchsuchung gleicht"?

Zu 23.
In beiden Fällen kommt sog. Remote Forensic Software zum Einsatz, die sich je nach Maßnahme jedoch maßgeblich in ihren Funktionalitäten unterscheidet.

24. Wie wird der Verkauf von Spähsoftware deutscher Hersteller zum Eindringen in fremde Rechnersysteme an andere Regierungen seitens der Bundesregierung kontrolliert und welche Rolle spielt dabei deren mögliche Nutzung zur Verletzung von politischen und Menschenrechten?

Zu 24.

Die Ausfuhr derartiger Technik unterliegt grundsätzlich keiner Genehmigungspflicht. Sie ist nur dann ausfuhrgenehmigungspflichtig, wenn sie von Anhang I der VO (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck (EG-Dual-Use-VO) oder als besonders entwickelt für militärische Zwecke von Teil I Abschnitt A der Ausfuhrliste (Anlage zur Außenwirtschaftsverordnung) erfasst ist.

Bei der Prüfung, ob gegebenenfalls eine Genehmigung erteilt werden kann, beachtet die Bundesregierung die „Politischen Grundsätze der Bundesregierung für den Export von Kriegswaffen und sonstigen Rüstungsgütern" von 2000 und den „Gemeinsamen Standpunkt 2008/944/GASP des Rates der Europäischen Union vom 8. Dezember 2008 betreffend gemeinsame Regeln für die Kontrolle der Ausfuhr von Militärtechnologie und Militärgütern", die entsprechend auch für den Export von Dual-Use-Gütern gelten. Danach werden Exportgenehmigungen bei dem hinreichenden Verdacht des Missbrauchs zur inneren Repression oder zu sonstigen fortdauernden und systematischen Menschenrechtsverletzungen grundsätzlich nicht erteilt.

25. Stellt der Verkauf von Software zum Ausspähen von Passwörtern oder dem Eindringen in private Rechnersysteme an das ägyptische Innenministerium nach Ansicht der Bundesregierung eine Straftat wegen „Ausspähen und Abfangen von Daten" nach § 202a oder § 202b dar (bitte begründen)?

Zu 25.

Der Verkauf von Software, die zum Ausspähen von Passwörtern und zum Eindringen in private Rechnersysteme geeignet ist, stellt allein noch keine Straftat dar. Hierbei kommt es vielmehr auf den Einzelfall an.

Die Regelungen des § 202a StGB (Ausspähen von Daten) und § 202b StGB (Abfangen von Daten) setzen eine konkrete Handlung voraus. Das heißt, es ist erforderlich, dass die Software dazu genutzt wird, sich oder einem anderen unbefugt Zugang zu Daten zu verschaffen, die nicht für den Nutzer bestimmt sind und die gegen unberechtigten Zugang besonders gesichert sind (§ 202a StGB) oder dass sie genutzt wird, sich oder einem anderen unter Anwendung von technischen Mitteln nicht für den Nutzer bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage zu verschaffen (§ 202b StGB).

Der Verkauf von Software, die grundsätzlich für diese Taten geeignet ist, erfüllt daher keinen dieser Tatbestände. Es käme nur eine Strafbarkeit in Betracht, wenn es sich um eine strafbare Vorbereitungshandlung zu einer dieser Taten nach § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten) handelt.
Voraussetzung hierfür ist, dass der objektive Zweck der Software die Begehung einer der genannten Taten ist. Eine bloße Eignung des Programmes zur Begehung solcher Taten allein genügt nicht (sog. "dual-use-Programme", vgl. auch BVerfG 2 BvR 2233/07). Weiterhin muss der Betreffende durch seine Handlung (Herstellung, Verschaffen, Verkauf, Überlassen, Verbreiten) eine der genannten Straftaten vorbereiten.

26. Welche Schritte hat die Bundesregierung nach Bekanntwerden von Verkaufsabsichten von Spähsoftware der Firma Elaman an das ägyptische Innenministerium unternommen?

Zu 26.
Der Bundesregierung liegen keine eigenen Erkenntnisse zu Verkaufsabsichten dieses Unternehmens nach Ägypten vor.

27. Welche deutschen Firmen haben nach Kenntnis der Bundesregierung in den letzten fünf Jahren welche Regierungen mit Software zum Ausspähen von Passwörtern, dem Abhören rechnergestützter Kommunikation oder dem Eindringen in private Rechnersysteme beliefert?

Zu 27.
Aufgrund der bestehenden Datenbankstrukturen ist eine statistische Auswertung von Ausfuhren zu den angefragten Verwendungszwecken nicht möglich.

28. Wie steht die Bundesregierung zur Forderung einer weltweiten Ächtung von Software zum Ausspähen privater Rechnersysteme?

Zu 28.
Der Bundesregierung ist diese Forderung im Einzelnen nicht bekannt.