Deutscher Bundestag **Drucksache 17/5369**

17. Wahlperiode 05. 04. 2011

Kleine Anfrage

der Abgeordneten Andrej Hunko, Inge Höger, Niema Movassat und der Fraktion DIE LINKE.

Grenzüberschreitendes behördliches Ausspähen fremder Rechnersysteme („Governmental Hacking“)

Spätestens seit 2008 wurden mehrere Initiativen bekannt, innerhalb von EU-Institutionen „Maßnahmen zur Erleichterung von Ferndurchsuchungen“ (Ratsdokument 13567/08) zu etablieren. Erst in einer späteren Form wurden diese mit der Formulierung „sofern diese nach nationalem Recht vorgesehen sind“ eingeschränkt (Ratsdokument 15569/08). Die Initiativen mündeten im Vorschlag, eine „Partnerschaft zwischen der Polizei und dem privaten Sektor“ zu befördern (Pressemitteilung des Rates vom 27. November 2008). In einer Pressemitteilung vom 27. November 2008 „ermutigt“ der Präsident der Europäischen Kommission José Manuel Barroso diese beiden „Parteien“ zum „besseren Informationsaustausch über Ermittlungsmethoden und Entwicklungstrends“ und dazu „auf das Mittel der Ferndurchsuchung zurückzugreifen“. Die Maßnahmen auf EU-Ebene spezifizieren nicht zwischen sogenannter Quellen-Telekommunikationsüberwachung zum Abhören von Kommunikation bzw. Erstellen von Screenshots oder dem Durchsuchen des ausgespähten Rechnersystems.

In der Antwort auf die Kleine Anfrage (Bundestagsdrucksache 17/3143) erklärte die Bundesregierung, das deutsche Bundeskriminalamt (BKA) führe keine Statistiken darüber, ob von Europol, Interpol Wiesbaden oder anderen Behörden außerhalb Deutschlands gelieferte Informationen, womöglich auf „Ferndurchsuchungen“ beruhen. Noch nie hätten demgegenüber deutsche Behörden ihre Zustimmung zu „Ferndurchsuchungen“ von in Deutschland befindlichen Rechnern durch Ermittlungsteams anderer Länder gegeben.

Nach Presseberichten über dubiose Methoden von Landespolizeien zum Einbringen von sogenannten Trojaner-Programmen in private Rechner zum Abhören von Kommunikation hat die 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 eine Presseerklärung hierzu herausgegeben. Die Konferenz macht darauf aufmerksam, dass diese Ermittlungsmethode „in der Vorgehensweise einer Online-Durchsuchung gleicht“, da auch ein Zugriff auf gespeicherte Inhalte möglich sei. Die Datenschutzbeauftragten monieren hierfür das Fehlen „normenklarer gesetzlicher Regelungen“. Der Gesetzgeber solle daher „die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts“ klären.

In seinem halbjährlichen Brainstorming zu neuen Überwachungs- und Kontrollmaßnahmen hatte der EU-Anti-Terrorismus-Koordinator (ATK) im September 2010 die Festlegung eines „gemeinsamen justiziellen Rahmens für bestimmte Ermittlungstechniken“ gefordert und sich explizit auf „Online-Durchsuchungen“ bezogen (Ratsdokument 13318/1/10). Die Bundesregierung bezeichnet die

Ausführungen des Terrorismusbeauftragten zwar als seine „persönlichen Handlungsempfehlungen“. In einer späteren Mitteilung wird sein Vorschlag dennoch im März 2011 als „Follow-up“ aufgegriffen (Ratsdokument 5764/11) und als Gesetzgebungsinitiative anvisiert („Work to improve mutual awareness of good practises and draw up model agreements, and then establish a common juridical framework for certain investigative techniques such as the use of undercover agents and informers, or online searches“). Auffällig ist die Ineinssetzung von „Onlinedurchsuchungen“ mit dem Einsatz verdeckter Ermittlungen.

Ein Vermerk des EU-Rates vom 25. März 2010 enthält zudem die Anregung, den Austausch mit anderen „europäischen Einrichtungen“ auszubauen (Ratsdokument 5957/2/10 REV 2). Genannt werden „EMSI, CEPOL, Eurojust, Europol, ENISA“ sowie „Interpol, VN usw.“. Der Austausch soll sich vor allem um „neue Technologien“ drehen. Zudem solle die „Verwendung von computergestützten Ermittlungsinstrumenten durch Polizei, Justiz und forensische Dienste in ganz Europa“ ausgebaut werden und hierfür mit den „etablierten Einrichtungen“ ECTEG, Interpol, International Association for Computer Information Systems „oder anderen ähnlichen privaten und öffentlichen Organisationen“ zusammengearbeitet werden.

In ihrer Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 17/3143 hatte die Bundesregierung auf das Übereinkommen des Europarates über Computerkriminalität vom 23. November 2001 („Cybercrime-Konvention“) hingewiesen, das in Deutschland am 1. Juli 2009 in Kraft getreten ist. Die Konvention bildet demnach die rechtliche Grundlage zum staatlichen Eindringen in fremde Rechnersysteme im Rahmen der internationalen Rechtshilfe. Hingewiesen wird in der Antwort auf den Artikel 19 des Europol-Ratsbeschlusses, der ähnliche Formulierungen enthält wie die Mitteilungen des Rates zu Ferndurchsuchungen. Jede Vertragspartei ist laut Bundesregierung demnach „verpflichtet, die in ihrem Hoheitsgebiet vorhandenen, von einer Durchsuchung im Hoheitsgebiet einer anderen Vertragspartei betroffenen Daten durch die Gewährung des Zugriffs rasch und unmittelbar zur Verfügung zu stellen“.

Nach Bekanntwerden von wenigstens vorbereitenden Maßnahmen zur Lieferung von Software zum Eindringen in entfernte Rechner an das ägyptische Innenministerium und die Verwicklung der Münchener Firma Elaman GmbH in dem zweifelhaften Vorgang wird in netzpolitischen Kreisen die weltweite Ächtung von sogenannten Trojaner-Programmen gefordert. Fraglich ist, ob der Verkauf der Software nicht als Hilfe zum „Ausspähen und Abfangen von Daten“ verstanden werden kann, das gemäß § 202a oder § 202b des Strafgesetzbuchs (StGB) strafbar ist.

Wir fragen die Bundesregierung:

1. Welche Initiativen wurden auf EU-Ebene seit 2007 in strafprozessualer sowie juristischer Hinsicht ergriffen, um „Maßnahmen zur Erleichterung von Ferndurchsuchungen“ voranzutreiben?
2. Welche legislativen oder operativen Maßnahmen wurden für die Zukunft vorgeschlagen oder anvisiert, und welche Haltung hat die Bundesregierung hierzu eingenommen?
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?
4. Welche Arbeitsgruppen existieren bei welchen EU-Agenturen bzw. EU-Institutionen (auch SitCen – EU Joint Situation Center und ESVP – Europäische Sicherheits- und Verteidigungspolitik) zur Entwicklung von „Ferndurchsuchungen“ oder ähnlicher Initiativen, und wie sind deutsche Behörden daran beteiligt?

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

   Welche Einzelheiten sind der Bundesregierung hierzu bekannt?
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 auszuspähen?

   Welche Einzelheiten sind der Bundesregierung hierzu bekannt?
9. Hat der ATK inzwischen eine „nähere Erläuterung“ seiner „Empfehlungen“ vom September 2010 vorgelegt, und welchen Inhalt hat diese bezüglich der Entwicklung von „Maßnahmen zur Erleichterung von Ferndurchsuchungen“?

   Falls nein, wann ist mit der Erläuterung zu rechnen?
10. Wie bewertet die Bundesregierung die vom ATK aufgeworfenen Forderungen nach Änderungen der Rechtsordnung bezüglich des behördlichen Eindringens in fremde Rechnersysteme?
11. Wie bewertet die Bundesregierung das „Follow-up“ des Brainstormings des ATK (Ratsdokument 5764/11), das unter anderem eine Gesetzgebungsinitiative zu „Onlinedurchsuchungen“ anvisiert?
12. Welche Haltung nimmt die Bundesregierung in den Diskussionen zum Ratsdokument 5764/11 ein?
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?
14. Was ist damit gemeint, wenn eine „Partnerschaft zwischen der Polizei und dem privaten Sektor“ befördert werden soll, die im Ratsdokument 15569/08 vom Präsident der Europäischen Kommission aufgefordert werden „auf das Mittel der Ferndurchsuchung zurückzugreifen“?
15. Welche Initiativen wurden bezüglich dieser „Partnerschaft zwischen der Polizei und dem privaten Sektor“ bislang ergriffen?
16. Welchen Inhalt hat die Tagung „Forensic Science relating to Counter Terrorism“, die vom 14. bis 17. Juni 2011 in Polen stattfindet, bezüglich der Weiterentwicklung des behördlichen grenzüberschreitenden Ausspähens fremder Rechnersysteme?
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?
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 frü-

here Bundesminister des Innern, Dr. Wolfgang Schäuble, gemäß der Bundestagsdrucksache 16/3231 in einer Unterlage für den Haushaltsausschuss des Deutschen Bundestages unter der Überschrift „Online-Durchsuchung“ ausführt (bitte hinsichtlich etwaiger verschiedener Projekte erläutern)?

19. Welches „hierfür notwendige Instrumentarium“ ist seitdem, wie vom zwischenzeitlich entlassenen früheren Staatssekretär im Bundesministerium des Innern, August Hanning, ausgeführt, entwickelt worden?

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?

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?

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“?

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

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?

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 StGB dar (bitte begründen)?

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

27. Welche deutsche 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?

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

Berlin, den 5. April 2011

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333