Kleine Anfrage zur schriftlichen Beantwortung mit Antwort

Anfrage der Abgeordneten Maximilian Schmidt, Petra Emmerich-Kopatsch, Hans-Dieter Haase, Immacolata Glosemeyer, Dr. Alexander Saipa, Mustafa Erkan, Kathrin Wahlmann und Wiard Siebels (SPD), eingegangen am 07.01.2014

TAT-14-Landungspunkt Norden: Was ist über die Ausspähung des wichtigsten deutschen Übersee-Datenkabels bekannt?

Über das 2001 in Betrieb genommene Transatlantische Telefonkabel Nr. 14 (Transatlantic Telecommunications Cable no. 14, kurz: „TAT-14“) wird ein Großteil des Telekommunikations- und Datenverkehrs zwischen Europa und den Vereinigten Staaten von Amerika abgewickelt. Der Transport erfolgt auf zwei Routen im Ringverkehr, wobei eine Trasse von Norden in Ostfriesland über Blaabjerk (Dänemark) nach Manasquan und Tuckerton (New Jersey) führt; eine weitere Route verläuft von Norden über Katwijk (Niederlande), Saint-Valéry-en-Caux (Frankreich) und Bude (Großbritannien) ebenfalls durch den Atlantik nach New Jersey, USA. Nach bekannt gewordenen Unterlagen des US-Heimatschutzministeriums wird TAT-14 mit dem Landungspunkt Norden auf Rang 1 der „kritisch wichtigen Infrastruktur“ in der Bundesrepublik Deutschland genannt[1]. Neben TAT-14 enden in Norden auch weitere wichtige Datenkabel, so u. a. SEA-ME-WE 3, das Deutschland mit Asien und Australien verbindet.

Im Rahmen der Berichterstattung über die Abhörpraxis der NSA, des britischen GCHQ und weiterer Dienste wurde darauf verwiesen, dass diese Kabelverbindung als wesentliches Element für die Abschöpfung eines erheblichen Anteils der in Rede stehenden Kommunikationsdaten im Rahmen des Programms „Tempora“ genutzt wird. So schreibt etwa die *Süddeutsche Zeitung* nach gemeinsamer Recherche mit dem Norddeutschen Rundfunk am 25. Juni 2013: „Das Überwachungsprogramm ‚Tempora’ ist nach Angaben von Snowden ‚schlimmer’ als das jüngst bekannt gewordene ‚Prism’-Programm der USA. So soll sich der britische GCHQ heimlichen Zugang zu mehr als 200 Glasfaserkabeln weltweit verschafft haben - darunter auch TAT-14.“

Laut einem Bericht von *Focus online* vom 25.06.2013[2] wurde das Kabel in Bude, Cornwall, vom britischen Geheimdienst GCHQ angezapft und wurden die Daten über einen Zeitraum von einem Monat vollständig kopiert und gespeichert, um die Auswertung durch Geheimdienste zu ermöglichen. So sollen die Daten durch das GCHQ in Zusammenarbeit mit der NSA durch ca. 550 Analysten ausgewertet worden sein.

Vor diesem Hintergrund fragen wir die Landesregierung:

1. Wie gestaltete sich konkret das seinerzeitige Genehmigungs- und Errichtungsverfahren für TAT-14, wie ist das laufende Betriebsverfahren geregelt, und inwiefern war die Landesregierung daran beteiligt?

2. Ist der Landesregierung die Überwachungstätigkeit ausländischer Dienste über TAT-14 seit dem Errichtungsjahr 2001 bekannt geworden, wie wird diese bewertet, und sind Dienste des Landes oder der Bundesrepublik daran beteiligt gewesen?

3. Welche Maßnahmen wurden und werden künftig ergriffen, um die grundgesetzlich gewährleisteten Datenschutzrechte deutscher Bürgerinnen und Bürger zu schützen und für den Standort Niedersachsen schädigende Wirtschaftsspionage auszuschließen?

(An die Staatskanzlei übersandt am 10.01.2014 - II/725 - 560)

[1] vgl. http://wikileaks.org/cable/2009/02/09STATE15113.html

[2] vgl. http://www.focus.de/digital/internet/tid-32028/spionageprogramm-tempora-wieso-das-ostfriesische-staedtchen-norden-im-zentrum-des-spionageskandals-steht_aid_1025625.html

Antwort der Landesregierung

Niedersächsisches Ministerium
für Inneres und Sport
- 55-098-S-530006-1/14 -

Hannover, den 10.02.2014

Die gängige Abhörpraxis der USA und Großbritanniens - neben Kanada, Australien und Neuseeland - wurde bereits im Jahr 2001 durch den vom Europäischen Parlament eingesetzten Ausschuss über das Abhörsystem Echelon[3] dokumentiert.

Nach dem Abschlussbericht des Ausschusses bedarf es keines besonderen zusätzlichen Beweises, dass die fünf sogenannten ECHELON-Staaten (informell auch als „Five Eyes“ bezeichnet) durch ihre Auslandsdienste Kommunikation abhören. Aus jedem einzelnen dieser Staaten lassen sich bei Satellitenkommunikation Teile der Nachrichtenverkehre abgreifen, die für Empfänger im Ausland bestimmt sind.

Seinerzeit wurde auch die Frage der Überwachung kabel- und radiowellengebunder Kommunikation durch diese Staaten aufgeworfen, wobei zu diesem Zeitpunkt hierfür keine stichhaltigen Beweise gefunden werden konnten.

Da aber die mutmaßliche Überwachung des Datenverkehrs, der über (See-)Kabel erfolgt, analoge Rückschlüsse auf die Feststellungen zur Überwachung des Datenverkehrs, der via Satellit erfolgt, zuließ, warnt der Wirtschaftsschutz im Niedersächsischen Verfassungsschutz seitdem in seinen Vorträgen zur Sensibilisierung der Wirtschaft kontinuierlich vor den Gefahren durch solche Abhöraktivitäten.

Im Juni vergangenen Jahres sind erste Hinweise auf weitere, bisher nicht öffentlich bekannte nachrichtendienstliche Aktivitäten des US-amerikanischen Nachrichtendienstes NSA (National Security Agency) veröffentlicht worden.

Die Berichterstattungen thematisierten u. a. angebliche Aktivitäten der NSA zur Datenspionage durch technische Aufklärung der Internetknotenpunkte.

Deutschland wurde in diesem Zusammenhang als eines der Länder aufgeführt, das als ein Hauptoperationsgebiet der NSA gelte.

In der Folge wurden in den Medien auch ähnlich lautende Vorwürfe gegen den britischen Nachrichtendienst GCHQ (Government Communications Headquarters) erhoben.

In diesem Zusammenhang ist auch die Seekabelendstelle des Transatlantic Telecommunications Cable no. 14 (TAT-14) in Norden, Landkreis Aurich, in den Fokus der Medien geraten.

TAT-14 wird von einem internationalen Konsortium von 50 Telefongesellschaften, darunter auch die Deutsche Telekom, betrieben und finanziert.

Dies vorausgeschickt, beantworte ich die Anfrage namens der Landesregierung wie folgt:

Zu 1:

Für die Errichtung und den Betrieb des Unterwasserkabels TAT-14 im Bereich des Festlandsockels der deutschen Nordsee bis zur 12-Seemeilen-Grenze hat das heutige Landesamt für Bergbau, Energie und Geologie (LBEG) eine bergrechtliche Genehmigung auf der Grundlage von § 133 Abs. 1 Nr. 1 Bundesberggesetz erteilt. Entsprechend dieser Rechtsgrundlage bleibt diese Genehmigung auf die Regelung der mit diesem Vorhaben verbundenen bergbaulichen Aspekte beschränkt.

[3] **Echelon** ist der Name des Spionagesystems zum Abhören bzw. zur Überwachung von **über Satellit** geleiteten privaten und geschäftlichen Telefongesprächen, Faxverbindungen und Internet-Daten.

Die Genehmigung für die Errichtung des Kabels TAT-14 hat das LBEG am 27. Januar 2000 erteilt (AZ.: -20.3-03/00-W6005 Bh.7.0-I) erteilt. Die Regelungsinhalte bezogen sich dabei auf eine technisch einwandfreie Durchführung der Verlegung sowie die Minimierung von Unfallrisiken für die Beschäftigten. Die Genehmigung für den Betrieb des Kabels TAT-14 wurde am 6. März 2001 erteilt (AZ.: -20.3-15/00-W 6005 Bh.7.0-II-). Die Nebenbestimmungen dieser Betriebsgenehmigung enthalten keine Detailvorgaben, zeigen jedoch den bergrechtlichen Rechtsrahmen für einen technisch sicheren Betrieb und für eventuell erforderliche nachträgliche Bedingungen und Auflagen auf, z. B. im Falle einer Beschädigung des Kabels.

Im diesen bergrechtlichen Genehmigungsverfahren ist eine unmittelbare Beteiligung der obersten Landesbehörden nicht vorgesehen.

Hinsichtlich der Benutzung der Gewässer über dem Festlandsockel und des Luftraums über diesen Gewässern war ferner eine Genehmigung gemäß § 133 Abs. 1 Nr. 2 Bundesberggesetz erforderlich. Diese hat das Bundesamt für Seeschifffahrt und Hydrographie in Hamburg erteilt.

Zu 2:

Nachrichtendienste legen naturgemäß Details ihrer Arbeit nicht offen. Es gibt deshalb auch keine offizielle Erklärung dieser Dienste zu etwaigen „Spähprogrammen“ wie PRISM und TEMPORA.

Die Arbeit der in Rede stehenden Nachrichtendienste der USA und Großbritanniens wird auf der Grundlage von Gesetzen dieser Länder wahrgenommen. Diese Gesetze beschreiben sowohl Zweck als auch Vollmachten nachrichtendienstlicher Aktivitäten.

Es steht außer Frage, dass in den beiden benannten Staaten die zivile Kommunikation abgehört wird, die in das eigene Territorium hinein und aus diesem heraus geht.

So hat das Vereinigte Königreich im „Intelligence Service Act 1994“ ausdrücklich Spionageaktivitäten des heimischen Nachrichtendienstes gesetzlich verankert.

Es ist besonders darauf hinzuweisen, dass diese Spionagehandlungen namentlich auch für die Zwecke der Wirtschaftsspionage („economic well-being of the United Kingdom“) legitimiert worden sind.

Eine vergleichbare gesetzliche Legitimation ist für die Nachrichtendienste der USA mit dem „Protect America Act of 2007“ geschaffen worden.

Hier beziehen sich die Aktivitäten der nachrichtendienstlichen Erkenntnisgewinnung auf Personen außerhalb der USA und ermächtigen dazu, auch Internetprovider für sich in Anspruch zu nehmen.

Bis zu den Veröffentlichungen um den ehemaligen NSA-Mitarbeiter Edward Snowden gab es für die hiesige Spionageabwehr keine konkreten Anhaltspunkte, dass die NSA oder die GCHQ in Deutschland intensiv Aufklärung betreiben.

Es gibt in der Seekabelendstelle Norden/Niedersachsen keine erkennbaren Hinweise dafür, dass - wie verschiedene Medien berichteten - an diesem Übergabepunkt fremde (oder deutsche) Nachrichtendienste den Datenstrom des Überseekabels TAT-14 zu Überwachungszwecken ausleiten. Eine Überwachung der Kommunikation, die über dieses Seekabel erfolgt, an der Anlandungsstelle des Kabels in Bude (Großbritannien) und/oder den Endstellen in Manasquan und Tuckerton (beide USA) dürfte indes sehr wahrscheinlich sein.

Zu 3:

Die Spionageabwehr des Bundesamts für Verfassungsschutz (BfV) bearbeitet nachrichtendienstliche Aktivitäten fremder Staaten gegen Deutschland. Ziel ist dabei die Beendigung jeglichen unerlaubten nachrichtendienstlichen Agierens fremder Staaten in Deutschland. In diesem Zusammenhang untersucht das BfV auch die aktuellen Spionagevorwürfe gegen die USA und Großbritannien. Im Rahmen der Sachverhaltsaufklärung, die von dort bislang noch nicht abgeschlossen werden konnte, sind bisher keine Rechtsverstöße im Geltungsbereich des Grundgesetzes festgestellt worden.

In punkto Abwehr von Wirtschaftsspionage steht der Arbeitsbereich Wirtschaftsschutz des niedersächsischen Verfassungsschutzes als neutraler Dienstleister der niedersächsischen Wirtschaft seit

Langem beratend zur Seite. Er berät diese Unternehmen insbesondere in den Themen der Wirtschafts- und Industriespionage sowie der Sicherheit in der Informations- und Kommunikationstechnologie. Im Rahmen seiner bislang 13-jährigen Tätigkeit hat der Wirtschaftsschutz mehr als 6 000 Unternehmen mit sicherheitsrelevanten Informationen erreicht. Die Beratungen haben das Ziel, die Unternehmen über Gefahren zu sensibilisieren, Sicherheitsmaßnahmen zu initiieren und durch Prävention Schäden zu vermeiden und zu reduzieren.

Zurzeit werden gut 700 innovative und technologieorientierte Unternehmen und rund 250 Unternehmen im Geheimschutzverfahren[4] als feste Partner betreut. Schwerpunkte bilden dabei individuelle Beratungen vor Ort, Vorträge und Tagungen u. a. zur Cybersicherheit.

Das Vertrauen als wichtiger Faktor in der Zusammenarbeit zwischen den Sicherheitsbehörden und der Wirtschaft wurde in den letzten Monaten durch die Enthüllungen von Edward Snowden beeinträchtigt. Ungeachtet dieser Berichterstattungen werden Cyberattacken, also das Ausnutzen von Informations- und Kommunikationstechnologien für Angriffe gegen Unternehmen zum Zwecke der Wirtschaftsspionage und Wirtschaftskriminalität, in der Zukunft eine immer stärkere Rolle spielen.

Der niedersächsische Verfassungsschutz und das LKA werden ihre Arbeitsansätze im Bereich dieser Themenstellung intensivieren.

Boris Pistorius

[4] Das **Geheimschutzverfahren** in der Wirtschaft basiert im Wesentlichen auf dem „Handbuch für den Geheimschutz in der Wirtschaft“ (GHB), herausgegeben vom Bundesministerium für Wirtschaft und Energie (BMWi). Es widmet sich nicht dem Schutz von Firmengeheimnissen, sondern kommt regelmäßig dann zur Anwendung, wenn ein Unternehmen im Rahmen eines öffentlichen Entwicklungs- oder Produktionsauftrages mit Verschlusssachen befasst werden muss.

(Ausgegeben am 18.02.2014)