Kleine Anfrage zur schriftlichen Beantwortung
mit Antwort der Landesregierung
- Drucksache 17/5296 -

Darknet - Die dunkle Seite des Internets?

Anfrage der Abgeordneten Marco Brunotte, Kathrin Wahlmann und Maximilian Schmidt (SPD) an die Landesregierung,
eingegangen am 29.02.2016, an die Staatskanzlei übersandt am 02.03.2016

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung vom 31.03.2016,
gezeichnet

Boris Pistorius

Vorbemerkung der Abgeordneten

Die Anzahl der Delikte im Bereich Cyberkriminalität steigt stetig. Neben dem Diebstahl von Zugangsberechtigungen, der Computersabotage, dem Ausspähen von Daten oder dem Phishing im Onlinebanking hat sich in den vergangenen Jahren eine weitere Tendenz herauskristallisiert: der Handel im Darknet.

Das Bundeskriminalamt geht davon aus, dass das „Hidden Web“ rund 90 % des gesamten Internets umfasst. Es ist somit weitaus größer als der auffindbare Teil. Ein kleiner Teil des Hidden Webs ist das Darknet.

Das Darknet ist ein versteckter Dienst, der beispielsweise über das TOR-Netzwerk angesteuert werden kann. Es ist nicht über Suchmaschinen oder den einfachen Aufruf des Internetbrowsers erreichbar. Die IP-Adresse wird über mehrere Server verschleiert und ermöglicht eine weitreichende Anonymisierung der Verbindungsdaten.

Das Darknet ist aber auch z. B. für Oppositionelle in Diktaturen, Whistleblower, Journalisten und andere ein wichtiger Weg, Informationen auszutauschen, um sich staatlicher Überwachung und Verfolgung zu entziehen.

Über digitale Währungen (Bitcoins) ermöglichen Handelsplattformen den anonymen Usern den Kauf von zahlreichen illegalen Gütern. Hier gibt es Drogen, Kinderpornos, Auftragskiller, Waffen, gefälschte Papiere und vieles mehr.

Im Jahr 2015 wurde Ross Ulbricht in den USA zu einer lebenslangen Haft verurteilt. Er ist Gründer der Untergrundhandelsplattform „Silk Road“, die als Zentrum des Online-Drogenhandels galt. Drogenschäfte und gefälschte Papiere im Volumen von etwa 200 Millionen US-Dollar seien innerhalb mehrerer Jahre über die Plattform abgewickelt worden.

Auch in Niedersachsen sind Fälle von Kriminalität im Darknet bekannt geworden. Ein 23-jähriger Mann wurde nach Ermittlungen der Staatsanwaltschaft Verden im Jahr 2013 festgenommen. Unter dem Decknamen „Kron0s“ soll er im Darknet Betäubungsmittel und Marihuana verkauft haben. Auch wegen des Verdachts auf Waffenhandel wurde gegen ihn ermittelt.

Im Oktober 2015 wurde ein 22-jähriger Mann vor dem Landgericht Hannover zu einer mehrjährigen Haftstrafe verurteilt. Er hatte sich über das Darknet mit einem Belgier zur Vergewaltigung seines 11-jährigen Sohnes verabredet und die Tat ausgeführt. Auf die Spur kamen ihm australische Ermittler, die im Darknet auf der Suche nach Pädophilen ermittelten.

Vorbemerkung der Landesregierung

Das Deep Web, auch Hidden oder Invisible Web, ist der Teil des Internets, der von den meisten gebräuchlichen Suchmaschinen nicht gefunden wird. Die Informationen im Deep Web bestehen zu einem großen Teil aus umfassenden (Fach-)Datenbanken wie z. B. Bibliothekskatalogen oder wissenschaftlichen Daten (beispielsweise Physik, Chemie, Medizin, Klimaforschung u. a.). Die Datenbanken des Deep Web benötigen in der Regel spezielle Anfragen, die von den herkömmlichen Web-Crawlern (Programme der Suchmaschinen zur Analyse von Internetseiten) der gebräuchlichen Suchmaschinen nicht verarbeitet werden. Allgemein entscheidet der Ersteller von Webinhalten grundsätzlich selbst darüber, ob und welche Teile seiner Seiten von den Web-Crawlern gefunden werden sollen.

Eine spezielle Form des Deep Web ist das Darknet. Der Begriff steht nicht per se für ein kriminelles Netz, sondern vielmehr für eine Form der technischen Ausgestaltung (Peer to Peer, d. h. Knoten zu Knoten) zur Gewährleistung eines hohen Maßes an Privatheit und Anonymität. Die derzeit verbreitetste technische Lösung für einen Zugang in diesen Teil des Internets ist die Nutzung des TOR-Netzwerks (The Onion Routing). Die Nutzung ist durch die einfache Installation eines TOR-Browsers möglich. Dieser erlaubt echtzeit-anonymisiertes Surfen über sogenannte TOR-Netzwerknoten. Der derzeitige Entwicklungsstand des TOR-Netzes bietet vor allem zwei Kernfunktionen: das sogenannte anonyme Surfen sowie das Nutzen versteckter Dienste (sogenannte hidden services), gekennzeichnet durch die Endung .onion. Eine Deanonymisierung und damit Identifizierung wird in diesem Netzwerk verhindert. Darüber hinaus wird über TOR die Nutzung versteckter Dienste angeboten, zu denen man ebenfalls anonymisiert gelangt.

In einer aktuellen Veröffentlichung „Cryptopolitik and the Darknet“[1] des International Institute for Strategic Studies (IISS) vom 1. Februar 2016 berichten die beiden Wissenschaftler des Department of War Studies am King’s College London, Daniel Moore & Thomas Rid, über ihre Studien zum Darknet. Zu der Frage der Notwendigkeit von Diensten zur Unterstützung der Privatheit und des Datenschutzes wird ausgeführt, dass beispielsweise Journalisten verschiedener Medien den TOR-Netzwerk-Service nutzen, um Informationen von Whistleblowern zu erlangen. Der Vorteil dieser Services wird darin gesehen, dass man den durch das TOR-Verfahren geschützten Kommunikationsraum nicht mehr über einen Ausgangsknoten (Exit-Node) verlassen muss, also ein weiterer technischer Angriffspunkt entfalle. Der dort inzwischen etablierte Whistleblower-Dienst „SecureDrop“ wird von einer Reihe namhafter Medien, z. B. Washington Post, The Guardian, Forbes, ProPublica usw., genutzt[2].

Die Wissenschaftler führen weiter aus, dass sie nach eigenen Angaben insgesamt 5 205 TOR-Webseiten analysiert haben. Davon konnten 2 723 bewertet werden, 1 547 Seiten davon wiesen illegale Inhalte auf. Die Verfasser kommen daher zu dem Ergebnis einer „überwältigen Präsenz illegaler Inhalte im TOR-Darknet“.

Über das Deep Web hinaus haben die technischen Entwicklungen und die drastische Ausweitung der Internetkriminalität in den letzten Jahren die Strafverfolgungsbehörden vor neue und besondere Herausforderungen gestellt. Diese haben darauf reagiert und sich auf das neue Kriminalitätsfeld eingestellt.

Auf justizieller Ebene sind landesweit Schwerpunktstaatsanwaltschaften für Kriminalität auf dem Gebiet der Informations- und Kommunikationstechnik (IuK) eingerichtet worden. In jedem Bezirk der drei niedersächsischen Generalstaatsanwaltschaften Braunschweig, Celle und Oldenburg gibt es seit dem 1. Januar 2012 eine Schwerpunktstaatsanwaltschaft. Standorte sind Göttingen, Verden und Osnabrück.

Das Aufgabengebiet der bei der Generalstaatsanwaltschaft in Celle angesiedelten Zentralen Stelle Organisierte Kriminalität und Korruption (ZOK), die für Niedersachsen zentrale Beratungs-, Koordinierungs- und Unterstützungsaufgaben wahrnimmt, wurde bereits am 15. Juli 2011 auf den Bereich IuK-Kriminalität erweitert. Die drei IuK-Zentralstellen in Göttingen, Osnabrück und Verden ermitteln nicht nur niedersachsenweit, sondern führen zahlreiche bundesweite Sammelverfahren. Da das In-

[1] http://www.iiss.org/en/publications/survival/sections/2016-5e13/survival--global-politics-and-strategy-february-march-2016-44d5/58-1-02-moore-and-rid-9204, abgerufen am 10.03.2016

[2] https://en.wikipedia.org/wiki/SecureDrop, abgerufen am 10.03.2016

ternet keine Grenzen kennt, haben die Ermittlungen sehr häufig auch internationale Bezüge und erfordern zahlreiche Maßnahmen auf dem Gebiet der Rechtshilfe.

Das Justizministerium hat rechtzeitig erkannt, dass das Internet ständig neue Möglichkeiten für Straftäter eröffnet und neue Kriminalitätsphänomene schafft und deshalb entsprechend reagiert: Die IuK-Zentralstellen wurden im Jahr 2014 um insgesamt fünf Stellen personell verstärkt, um den Herausforderungen der sich stetig wandelnden Kriminalität in diesem Bereich künftig noch effektiver begegnen zu können.

Auf Seiten der Polizei wurde im Landeskriminalamt Niedersachsen bereits zum 1. August 2009 die Zentralstelle Cybercrime mit den Sachgebieten zur Analyse und Auswertung der Internetkriminalität, Ermittlungen Internetkriminalität und Anlassunabhängige Recherche in Datennetzen eingerichtet. Darüber hinaus hat die Polizei die Kompetenzen zur Bekämpfung spezieller, zumeist der organisierter Kriminalität zuzurechnenden Fällen oder von Banden begangener Fälle von Cybercrime in den Zentralen Kriminalinspektionen der Polizeibehörden gebündelt. In Ergänzung werden besondere Cybercrimedelikte in den Fachkommissariaten der Polizeibehörden bearbeitet.

Aktuell werden die Auswahlverfahren zur Einstellung von 22 zusätzlichen IT-Spezialistinnen/IT-Spezialisten für die Bekämpfung von Cybercrime in den Zentralen Kriminalinspektionen sowie für das Landeskriminalamt Niedersachsen durchgeführt. Diese Auswahlverfahren werden im März 2016 beendet sein.

Infolge der Neustrukturierung in Niedersachsen durch den Aufbau spezialisierter Ermittlungsgruppen bei den Polizeibehörden - maßgeblich bei den Zentralen Kriminalinspektionen und dem Landeskriminalamt Niedersachsen - und der gleichlaufenden Einrichtung spezialisierter operativer Zentralstellen bei den Staatsanwaltschaften in Göttingen, Osnabrück und Verden konnte erhebliche Expertise bei der Bekämpfung der Internetkriminalität, so auch bei den Ermittlungen im Darknet, gewonnen werden. Dieser Anstieg der Ermittlungskompetenz in Niedersachsen ist durch eine fortlaufende Fortbildung, stetigen Erfahrungsaustausch und eine enge Abstimmung zwischen Polizei und Staatsanwaltschaft möglich geworden.

1. Wie viele Strafverfahren mit Bezug ins Darknet wurden in den letzten fünf Jahren in Niedersachsen zu welchen Deliktsarten geführt?

Statistiken zu Strafverfahren mit einem Bezug zum sogenannten Darknet werden nicht geführt. Eine Aussage dazu, wie viele Strafverfahren mit Bezug ins Darknet mit welchen zugrundeliegenden Straftaten geführt worden sind, kann daher nicht getroffen werden. So ist beispielsweise bei dem Missbrauch von Kreditkartendaten nicht erkennbar, wie der Täter an diese Daten gekommen ist und ob er sie z. B. auf einem illegalen Marktplatz im Darknet erworben hat. Insoweit können keine Aussagen zur konkreten Anzahl entsprechender Strafverfahren in Niedersachsen getätigt werden.

Die Beantwortung der Fragen würde eine händische Einzelauswertung aller Verfahrensakten bei den niedersächsischen Staatsanwaltschaften für den entsprechenden Zeitraum erforderlich machen. Damit wäre ein Arbeitsaufwand verbunden, der ohne Zurückstellung der eigentlichen Aufgaben der Staatsanwaltschaften nicht möglich wäre und zudem im Rahmen der Beantwortung einer Kleinen Anfrage nicht geleistet werden kann.

Eine zahlenmäßige Erhebung wäre auch auf polizeilicher Seite mit einer aufwändigen, umfangreichen Behördenabfrage nicht durchführbar, da die Bezüge der in Niedersachsen bearbeiteten Strafverfahren zum Darknet in den polizeilichen Datenbanken nicht gesondert erfasst werden.

2. In wie vielen Fällen kam es nach der Anklage auch zu einer Verurteilung?

Über die Anzahl der in den letzten fünf Jahren erhobenen Anklagen und rechtskräftigen Verurteilungen können keine Angaben gemacht werden. Darüber hinaus wird auf die Antwort zu Frage 1 verwiesen.

3. Welche Ermittlungsmöglichkeiten hat das Land Niedersachsen im Darknet?

Durch die durchgehende Verwendung von Verschlüsselung und/oder Anonymisierungsdiensten, wie z. B. des TOR-Netzwerks, gestalten sich die Ermittlungen im Darknet überaus zeitintensiv und schwierig. „Klassische“ Maßnahmen - wie die Überwachung der Telekommunikation - führen in den seltensten Fällen zum Erfolg. Durch die systembedingte Anonymität der agierenden Personen im Darknet ist eine erfolgreiche Identifizierung meist nur möglich, wenn Spuren in das „offene“ Internet oder die reale Welt weisen.

Den niedersächsischen Strafverfolgungsbehörden stehen die durch die Strafprozessordnung vorgegebenen Ermittlungsinstrumente zur Verfügung. Bei den personellen Ermittlungen wird auf Grundlage der §§ 161, 163 StPO (nicht offen ermittelnder Beamter) beziehungsweise § 110 a StPO (verdeckter Ermittler) innerhalb von legendierten Kommunikationsbeziehungen zu den Tatverdächtigen gehandelt.

Im Bereich der technischen Ermittlungen stehen Serverüberwachungsmaßnahmen (§§ 100 a, 100 g StPO) und Durchsuchungsmaßnahmen (§§ 94, 95, 99 StPO) im Mittelpunkt. In diesem Zusammenhang ist anzumerken, dass nicht jede technisch zur Verfügung stehende Ermittlungsmöglichkeit auch rechtlich zulässig ist und somit durchgeführt wird.

4. Wie haben sich in den letzten fünf Jahren die technischen und personellen Ermittlungsmöglichkeiten des Landes Niedersachsen im Darknet verändert?

Es wird auf die Vorbemerkung und die Antwort zu Frage 3 verwiesen. Ergänzend ist anzuführen, dass bei der Abrufbarkeit von IP-Adressen die nahezu flächendeckend eingeführte NAT/NAPT-Technik (Networkadresstranslation bzw. Networkadressporttranslation), bei der eine IP-Adresse einer Vielzahl von Nutzern zugeordnet wird, die Strafverfolgungsbehörden vor besondere Schwierigkeiten stellt. Da bei sogenannten Ermittlungen im Darknet im Regelfall gegen organisierte, oftmals internationale Tätergruppen ermittelt wird, gestalten sich die Ermittlungen bei zunehmender Datenmenge und rasanter internationaler Beweglichkeit der Täter als zunehmend herausfordernd.

5. Gibt es zu Ermittlungen im Darknet einen bundesweiten oder internationalen Austausch?

Ja. Aufgrund der Tatsache, dass die Tätergruppierungen international aufgestellt sind, müssen erfolgreiche Ermittlungen zwangsläufig eine starke nationale und internationale Kooperation beinhalten. Dies ist der Fall, zumal ein wichtiges Initial für Ermittlungen im Darknet internationale Großoperationen sind, an denen die Bundesrepublik Deutschland teilnimmt. Genannt sei beispielsweise die Operation Onymous, an der sich für die Bundesrepublik Deutschland Hessen und Niedersachsen beteiligt haben. In der Folge hat dies auch in Niedersachsen zu Verfahren mit Bezug zum Darknet geführt.

Es steht zu erwarten, dass der Anteil internationaler konzertierter Aktionen im Darknet zukünftig ansteigen wird. So sind die niedersächsischen Ermittlungsbehörden eng untereinander, aber auch mit vergleichbaren Ermittlungsstellen im Bundesgebiet und den europäischen Institutionen wie Europol und Eurojust vernetzt. Zudem werden enge Beziehungen insbesondere zu den anderen europäischen Staaten und den G7-Staaten unterhalten. Dabei nehmen die Vereinigten Staaten von Amerika eine herausgehobene Stellung ein. Besondere Bedeutung kommt der Koordinierung durch Europol/Eurojust zu. Bundesdeutsche Ermittlungsbehörden, vorrangig das BKA, bemühen sich zudem um einen stärkeren und verstetigten Austausch, um Ermittlungen in diesem Bereich zu koordinieren.

Anlassbezogen werden auf Bundesebene zudem ermittlungsrelevante Informationen im Rahmen der polizeilichen Meldedienste ausgetauscht. Erfahrungen im Zusammenhang mit Ermittlungen im Darknet, die in den einzelnen Bundesländern gemacht wurden, werden darüber hinaus periodisch u. a. im Rahmen von Workshops und Tagungen ebenso ausgetauscht wie Erfahrungen mit internationaler Relevanz über das BKA.

6. Wie beurteilt die Landesregierung das Zahlungssystem Bitcoin?

Nach Artikel 3 Abs. 4 des Vertrags über die Europäische Union ist der Euro die geltende Währung der Europäischen Wirtschafts- und Währungsunion. Zudem regelt § 14 Abs. 1 des Gesetzes über die Deutsche Bundesbank, dass die auf Euro lautenden Banknoten das einzige uneingeschränkte gesetzliche Zahlungsmittel in der Bundesrepublik Deutschland sind.

Die Bundesanstalt für Finanzdienstaufsicht hat 2013 festgelegt, dass sie die Bitcoins rechtlich verbindlich als Finanzinstrumente in der Form von Rechnungseinheiten gemäß § 1 Abs. 11 Satz 1 des Kreditwesengesetzes (KWG) qualifiziert hat.

Nach Einschätzung bzw. Bewertung von Europol vom Oktober 2015 wird Bitcoin nicht nur im Darknet eingesetzt, sondern ebenso von Kriminellen für Straftaten wie Erpressungen und Geldwäsche genutzt. So wurde Glückspiel- und Finanzunternehmen mit Angriffen auf ihr Netzwerk gedroht. Gegen Zahlung von Summen zwischen 1 und 100 Bitcoin sollten sie sich „freikaufen“. Im Gegensatz zu einem Bankkonto ist bei einer Bitcoinadresse erst einmal unbekannt, wer ihr Inhaber ist. Bei Europol ist daher noch nicht abschließend bewertet, was die Regulierung von Bitcoins bzw. virtuellen Währungen angeht. Es ist unklar, wie Regeln gegenüber anonymen Nutzern durchgesetzt werden können.

7. Welche Erkenntnisse hat die Landesregierung über Geldwäsche durch Bitcoins?

In Niedersachsen sind in den vergangenen Jahren keine Geldwäschesachverhalte mit Bitcoin-Bezug bekannt geworden.

Die Nutzung von sogenannten Kryptowährungen wie Bitcoin wird - neben dem legalen Nutzen - im Bereich des Darknet auch zur Bezahlung von inkriminierten Waren eingesetzt. Durch die Pseudonymität des Bezahlvorgangs ist eine Rückbeziehung auf die Zahlungspartner mit den vorhandenen technischen und rechtlichen Mitteln nahezu ausgeschlossen. Dieser Umstand wird bewusst auch in Täterkreisen ausgenutzt, um inkriminierte Waren und Dienstleistungen auszutauschen beziehungsweise Zahlungsströme zu verschleiern.

8. Wie beurteilt die Landesregierung das Darknet im Zwiespalt zwischen Kommunikationsmittel für Oppositionelle in Diktaturen und Plattform für illegale Geschäfte?

Das Darknet bietet als spezielle Ausformung einer digitalen Kommunikationsstruktur Anonymität oder zumindest Pseudonymität für jeden Anwender. Aus Sicht der Strafverfolgungsbehörden wird dieser Raum auch durch organisierte Täterstrukturen zur Begehung oder Verabredung von Straftaten genutzt. Da im Darknet u. a. aufgrund technischer Herausforderungen zurzeit nur eingeschränkt ermittelt werden kann, sind die legitimen Nutzungsinteressen mit dem Interesse an effektiver Strafverfolgung auch in diesem Raum in Einklang zu bringen.

(Ausgegeben am 08.04.2016)