



DPoIG
DEUTSCHE POLIZEIGEWERKSCHAFT
im DBB

DPoIG • Dr.-Alfred-Herrhausen-Allee 12 • 47228 Duisburg

Präsidentin des Landtags
Nordrhein - Westfalen

Postfach 101143

40002 Düsseldorf



Landesverband NRW

Dr.-Alfred-Herrhausen-Allee 12
47228 Duisburg
Telefon (02065) 70 14 82
Telefax (02065) 70 14 83

info@dpolg-nrw.de
www.dpolg-nrw.de

Duisburg, 14. März 2016

Terrorbekämpfung stärken – Gesondertes digitales Kompetenzzentrum zur Bekämpfung, Verfolgung und Verhinderung terroristischer Aktivitäten in Nordrhein-Westfalen aufbauen
Schriftliche Anhörung von Sachverständigen durch den Innenausschuss des Landtags Nordrhein-Westfalen

Antrag der Fraktion der CDU - Drucksache 16/10303

Stellungnahme der DPoIG

1. Antrag der Fraktion der CDU

Der Antrag der Fraktion der CDU bezieht sich auf verschiedene Veröffentlichungen nach den terroristischen Anschlägen in Paris vom 13. November 2015, die darlegen, dass die Terroristen im Vorfeld der Anschläge Informationen über das Internet ausgetauscht haben. Ein Teil dieser Informationen/Hinweise sei dabei über soziale Netzwerke und Messenger-Dienste verbreitet worden. Eine rechtzeitige Weiterleitung der Inhalte „an eine zentrale Dienststelle zur weiteren Ermittlung bzw. Überprüfung“ hätte automatisch durch die Betreiber der entsprechenden Dienste erfolgen können. Außerdem würden sich die Terroristen zur eigenen Finanzierung so genannter Bitcoins bedienen, die im digitalen Netz verfolgbar seien.

Zur Sicherung der „freiheitlichen Lebensweise“ sei ein „digitales Kompetenzzentrum zur Terrorabwehr, welches international mit befreundeten Behörden bei der Ermittlung und Vereitelung von terroristischen Anschlägen kooperiert und effiziente Handlungs- und Entscheidungsstrukturen aufweist, wichtig.

2. Nationale Terrorismusbekämpfung

2.1. Allgemeines



Bereits heute ist die nationale Terrorismusbekämpfung in Deutschland gesetzlich geregelt. Hierzu zählt unter anderem das Terrorismusbekämpfungsgesetz (TBG), in dem die Zuständigkeit des Bundeskriminalamtes (BKA) und des Bundesamtes für Verfassungsschutz (BfV) geregelt wird. Im Vordergrund behandelt das TBG die Informationsgewinnung und den Informationsaustausch relevanter Daten zur Terrorismusbekämpfung.

Für die Interaktion der sicherheitspolitischen Akteure werden die Strukturen durch das Grundgesetz (GG), als eines der Organisationsprinzipien des Rechtsstaats, vorgegeben. Die Akteure der ausführenden Gewalt sind der Bundesnachrichtendienst (BND), der Verfassungsschutz, der Militärische Abschirmdienst (MAD) und die Polizei des Bundes und der Länder, wobei hier auf das Trennungsgebot nicht näher eingegangen werden soll. Im Mittelpunkt der Zusammenarbeit stehen der operative Informationsaustausch sowie die Aufklärung des islamistisch terroristischen Personenpotentials.

2.2. Nationale Regelungen

Das gemeinsame Internetzentrum (GIZ) wurde 2007 zur Beobachtung und Bewertung islamistischer Internetinhalte in Berlin eingerichtet. Hier arbeiten Vertreter des BfV, des BND, des MAD und der Generalbundesanwaltschaft eng zusammen. Aufgabe der Vertreter der am GIZ mitwirkenden Behörden ist die Beobachtung, Auswertung und Analyse von Veröffentlichungen mit islamistischen und jihadistischen Inhalten im Internet, um hierdurch frühzeitig extremistische und terroristische Strukturen und Aktivitäten zu identifizieren.¹

Der ständige Informationsaustausch mit den Landesbehörden ist gewährleistet.

Des Weiteren ist noch das gemeinsame Terrorismusabwehrzentrum (GTAZ) 2004 in Berlin als gemeinsame Kooperations- und Kommunikationsplattform von 40 nationalen Behörden aus dem Bereich der Inneren Sicherheit gegründet worden. Die Einrichtung des GTAZ erfolgte vor dem Hintergrund einer verstärkten Bedrohung durch den islamistischen Terrorismus. Folgende Behörden arbeiten gemeinsam innerhalb ihrer eigenen Kompetenzen: BfV, BKA, Generalbundesanwalt (GBA), Bundespolizei (BPol), Zollkriminalamt (ZKA), Bundesamt für Migration und Flüchtlinge (BAMF), MAD, Landesämter für Verfassungsschutz (LfV) und die Landeskriminalämter (LKÄ). Die Kooperation zwischen nachrichtendienstlichen und polizeilichen Institutionen und Akteuren trägt zum Erfolg des GTAZ bei. Hierzu wurden nachrichtendienstliche und polizeiliche Informations- und Analysestellen (NIAS und PIAS) gegründet.²

Weiterhin nahm das Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ) am 15. November 2012 seine Arbeit auf. Unter seinem Dach wird die Kooperation zwischen Polizei und Verfassungsschutz, zwischen Bund und Ländern in den Phänomenbereichen Rechtsextremismus/-terrorismus, Linksextremismus/-terrorismus, Ausländerextremismus, Spionageabwehr und Proliferation gebündelt. Ziel ist es, Fachexpertise aller Behörden unmittelbar zu bündeln und einen möglichst lückenlosen und schnellen Informationsfluss sicherzustellen. Beteiligt sind bisher folgende Behörden: BKA, BPol, Europol, GBA, ZKA, BfV, BND, MAD, BAMF, Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAfA), LKÄ sowie LfV.³

Am 16. Juni 2011 wurde offiziell in Bonn das Nationale Cyber-Abwehrzentrum (Cyber-AZ) gegründet. Angesichts der steigenden Cyber-Gefahren arbeiten die Bundesbehörden, die sich mit den relevanten Facetten dieses Themas beschäftigen, enger zusammen. Unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bilden

¹ <https://www.verfassungsschutz.de/de/arbeitsfelder/af-islamismus-und-islamistischer-terrorismus/gemeinsames-internetzentrum-giz>, Abfragedatum: 13.03.16

² <https://www.verfassungsschutz.de/de/arbeitsfelder/af-islamismus-und-islamistischer-terrorismus/gemeinsames-terrorismusabwehrzentrum-gtaz>, Abfragedatum: 13.03.16

³ <https://www.verfassungsschutz.de/de/das-bfv/getz>, Abfragedatum: 13.03.16



dort das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) und die Bundeswehr eine Einheit.⁴ In seiner Eröffnungsrede ging der damalige Bundesinnenminister Herr Friedrich auch auf das Ziel des Cyber-AZ ein: "Ziel ist es, die operative Zusammenarbeit der relevanten staatlichen Stellen zu optimieren und die Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle besser zu koordinieren."⁵

Beim BKA wird bereits seit 2003 die Forschungs- und Beratungsstelle Terrorismus / Extremismus (FTE) betrieben. Hier arbeiten Kriminalbeamte und Wissenschaftler aus unterschiedlichen sozialwissenschaftlichen Fachrichtungen zusammen und vereinen fallbezogene polizeiliche Auswertungen und Analysen mit professionellem Theorie- und Methodenwissen zu einem integrativen Ansatz, durch den neben wissenschaftlichem Output auch der praktische Bezug zur polizeilichen Arbeit erhalten bleibt. Die FTE forscht mit dem Ziel, die Effizienz von Anti-Terror-Maßnahmen stets zu verbessern und weiter zu entwickeln.⁶

2.3. LKA NRW

Beim Landeskriminalamt (LKA) NRW wurde im Jahr 2011 das Cybercrime-Kompetenzzentrum eingerichtet. Über die Zentrale Ansprechstelle Cybercrime (ZAC) sind rund um die Uhr Experten erreichbar, die die Anfragen anderer staatlicher Behörden, Institutionen und Verbände aus Forschung und Lehre sowie der Wirtschaft entgegennehmen, bearbeiten und steuern. Folgende Aufgaben werden darüber hinaus wahrgenommen: Grundsatzangelegenheiten und Prävention, Zentrales Informations- und Servicezentrum Cybercrime (ZISC), Zentrale Auswertungs- und Sammelstelle Kinderpornografie (ZASt), Zentrale Internetrecherche (ZIR), Ermittlungskommissionen (EK), Telekommunikationsüberwachung (TKÜ) und Ermittlungsunterstützung, Computerforensik.⁷

3. Auseinandersetzung mit der Forderung: „gesondertes digitales Kompetenzzentrum“

Grundsätzlich kann gesagt werden, dass eine umfassende Überwachung der weltweiten Kommunikation über das Internet nicht möglich erscheint. Nach einer aktuellen Online Studie der Sendeanstalten ZDF/ARD aus dem Jahr 2015⁸ nutzen allein in Deutschland täglich ca. 44,5 Millionen Menschen das Internet und allein zur Kommunikation werden dazu täglich ca. 42 Minuten aufgebracht. Nach einer Statistik, die in der Frankfurter Allgemeinen Zeitung (FAZ) am 02.03.2015 veröffentlicht wurde, finden innerhalb einer Minute im Internet weltweit ca. 4 Millionen Suchanfragen bei Google, 277.000 Tweets, 100.000 Freundschaftsanfragen bei Facebook statt, es werden ca. 204 Millionen E-Mails und 13,8 Millionen ausgehende Nachrichten über Whatsapp verschickt.⁹ Es ist davon auszugehen, dass sich diese Zahlen bis zum heutigen Datum erheblich gesteigert haben. Sicher ist davon auszugehen, dass auch Terroristen/Extremisten diese Kommunikationswege in Anspruch nehmen und Nachrichten austauschen. Die Strafverfolgungsbehörden und auch die Nachrichtendienste sind bestrebt, diese Informationen frühzeitig zu erhalten

⁴ <http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyberabwehrzentrum/cyberabwehrzentrum.html>, Abfragedatum: 13.03.16

⁵ <https://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2011/06/ncaz.html>, Abfragedatum: 13.03.16

⁶ http://www.bka.de/nn_206010/DE/ThemenABisZ/Deliktsbereiche/TerrorismusExtremismus/ForschungsstelleTerrorismusExtremismus/fte_node.html?_nnn=true, Abfragedatum: 13.03.16

⁷ http://www.polizei.nrw.de/lka/artikel_9167.html, Abfragedatum: 13.03.16

⁸ <http://www.ard-zdf-onlinestudie.de/index.php?id=541>, Abfragedatum: 13.03.16

⁹ <http://www.faz.net/aktuell/wirtschaft/wirtschaft-in-zahlen/grafik-des-tages-was-binnen-einer-minute-im-internet-passiert-13459083.html>, Abfragedatum: 13.03.16



und mögliche geplante Anschläge zu verhindern, die Täter dingfest zu machen und einer Strafverfolgung zuzuführen.

Eine verfahrensunabhängige Recherche im Internet darf jedoch nicht kleinteilig und zergliedert ausfallen, da die Gefahr besteht, dass bestimmte Ermittlungstätigkeiten an mehreren Orten parallel oder in zeitlichem Versatz durchgeführt werden. Dadurch wird die Personalressource unnötig belastet. Es ist sicher effektiver, diese Internetrecherchen an einer zentralen Stelle zusammenzuführen und zu koordinieren. Hierzu sind bereits umfangreiche Maßnahmen und Organisationsentscheidungen getroffen worden. Wichtig in diesem Arbeitsbereich ist es aus Sicht der DPoIG jedoch, gezielt ausgebildetes Personal in ausreichender Anzahl in diesen Bereichen einzusetzen. Dies gilt insbesondere auch bei den weiteren kriminalpolizeilichen Ermittlungen, die sich durch die Erkenntnisse der Recherchen ergeben können. Da sich diese Recherchen im Bereich des Terrorismus abspielen, wäre eine Bearbeitung dieser Fälle mit Tatort in NRW im LKA NRW sachlich geboten. Auch das Land NRW hat auf die Gefahr eines terroristischen Anschlags reagiert. So gab der Innenminister Herr Jäger am 15. Januar 2015 bekannt: „Nordrhein-Westfalen verstärkt Polizei und Verfassungsschutz. Dies ermöglicht eine noch effektivere Bekämpfung der Gefahr durch islamistische Terroristen. Bis 2017 werden deshalb insgesamt 385 zusätzliche Beamte eingestellt.“¹⁰ Die aktuellen Entwicklungen und Gefahren zeigen jedoch deutlich auf, dass die genannte Anzahl von Neueinstellungen nicht ausreichen wird, um diese Aufgabe zu erfüllen.

Wichtig in diesem Zusammenhang ist es, keine weiteren parallelen Strukturen aufzubauen. Innerhalb des Cybercrime-Kompetenzzentrums NRW gibt es bereits eine zentrale Internetrecherche (ZIR). Sicherlich gibt es hier Überschneidungen zu den genannten zentralen Einrichtungen der Terrorismusbekämpfung. Diese Überschneidungen lassen sich nicht gänzlich verhindern und sind in bestimmten Bereichen auch gewollt, um einen nicht kontrollierbaren Raum zu verhindern. Eine personelle Aufstockung der ZIR ist sinnvoll, um die Belange des Landes Nordrhein-Westfalen zu stärken. Eine Zusammenarbeit und intensiver Informationsaustausch mit den anderen Organisationen ist aus fachlicher Sicht zwingend geboten. Hierzu ist es wichtig, dass entsprechende Kommunikationswege geschaffen werden und wenn vorhanden, den aktuellen Erfordernissen anzupassen sind. Es darf kein Informationsdefizit der an der Terrorismusbekämpfung beteiligten Institutionen entstehen.

4. Bitcoin-Konten

Im Antrag der Fraktion der CDU wird auch über die Finanzierung der IS durch sogenannte Bitcoins gesprochen. So soll ein Konto der Terroristen im Wert von etwa \$ 3 Millionen entdeckt worden sein. Mit dieser Art der Finanzierung reagieren die Terroristen auf weltweit durchgeführte Finanzermittlungen der staatlichen Behörden. Die Finanzströme zu ermitteln ist eine effektive Möglichkeit, den internationalen Terrorismus zu bekämpfen und wertvolle Informationen für weitere Ermittlungshandlungen zu erhalten. Weiterhin können Konten eingefroren oder Geld/Wertanlagen beschlagnahmt und somit die finanziellen Möglichkeiten begrenzt werden. Aus diesem Grund machen kriminelle Banden und auch Terroristen die „Internetwährung“ Bitcoin für sich nutzbar. Die Rückverfolgung der Transaktionen, die nur Bruchteile von Sekunden dauern, wird durch die Wege im Internet erheblich erschwert oder verhindert. Bitcoin ist aktuell noch die weit verbreitete digitale Währung, die aber bereits Konkurrenz im digitalen Netz bekommt.¹¹

¹⁰ <http://www.mik.nrw.de/presse-mediathek/aktuelle-meldungen/aktuelles-im-detail/news/nrw-verstaerkt-die-terrorbekaempfung-mehr-personal-fuer-polizei-und-verfassungsschutz-innenminis.html>, Abfragedatum: 13.03.16

¹¹ <http://www.welt.de/wirtschaft/webwelt/article153228987/Das-ist-der-neue-grosse-Rivale-des-Bitcoin.html>, Abfragedatum: 13.03.16



Die Möglichkeiten der Transaktionen im Netz zeigen deutlich auf, dass zur Aufspürung, Rückverfolgung und Ermittlungen der Auftraggeber und Empfänger dieser Währung speziell ausgebildete Finanzermittler erforderlich sind, welche die gesamten Möglichkeiten der digitalen Welt kennen und wissen, wie diese funktioniert. Dies ist sicher ein Bereich, der noch einen erheblichen Nachholbedarf aufweist. Hier gilt es, entsprechend dotierte Stellen zu schaffen und auch Fachpersonal aus dem IT-Bereich zu verpflichten.

5. Weitere Forderungen

Weiterhin wird mit dem vorliegenden Antrag die Forderung aufgestellt, „Druck auf die Anbieter digitaler Kommunikationskanäle auszuüben, damit deren digitale Kommunikationsangebote nicht zu terroristischen Zwecken missbraucht werden.“ Außerdem wird die Forderung mit der „Schaffung eines rechtlichen Rahmens“ verbunden, die entsprechenden Daten „automatisch dem digitalen Kompetenzzentrum zur Terrorbekämpfung zu übermitteln, damit kurzfristig Ermittlungen aufgenommen werden können.“

Diese Forderungen an die Anbieter im digitalen Raum bestehen auch aus Sicht der Deutschen Polizeigewerkschaft. Es reicht nicht aus, wenn die Anbieter die entsprechenden Seiten oder Nachrichten sperren und somit für andere Personen nicht mehr erreichbar machen. Für eine effektive Strafverfolgung und eine wirkungsvolle Präventionsarbeit ist es erforderlich, die Verfasser zu identifizieren. Wenn es rechtlich möglich ist, sind Strafverfahren einzuleiten und die Straftaten konsequent zu verfolgen.

Eine solche Verfolgung ist nur möglich, wenn die Ermittlung der Verfasser grenzüberschreitend möglich gemacht wird. Das digitale Netz ist weltweit verfügbar und hält sich nicht an nationale Strafverfolgungsgrenzen. Hier ist ein Bereich, in dem durch politische Entscheidungen polizeiliche Ermittlungen erleichtert werden können.

Der Bereich der internationalen Kooperation zur Bekämpfung des Terrorismus wird aufgrund des eingeschränkten Gegenstandes des Antrages auf Ebene eines Bundeslandes an dieser Stelle nicht weiter beleuchtet.