Landeskriminalamt
Nordrhein-Westfalen

Landeskriminalamt Nordrhein-Westfalen,
Postfach 103452, 40025 Düsseldorf

Herrn
Daniel Sieveke MdL
Vorsitzender des Innenausschusses
des Landtags Nordrhein-Westfalen
Platz des Landtags 1

40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
16. WAHLPERIODE

STELLUNGNAHME
16/3603

A09

Aktenzeichen:
2 - 03.10

bei Antwort bitte angeben

KR Stascheit
Telefon 0211-939-2010
Telefax 0211-939-
matthias.stascheit
@polizei.nrw.de

Schriftliche Anhörung von Sachverständigen durch den Innenausschuss des Landtags Nordrhein-Westfalen
„Terrorbekämpfung stärken - Gesondertes digitales Kompetenzzentrum zur Bekämpfung, Verfolgung und Verhinderung terroristischer Aktivitäten in Nordrhein-Westfalen aufbauen“ Antrag der CDU; Drucksache 16/10303

Ihr Schreiben vom 16.02.2016

Anlage: - 1 -

Dienstgebäude:
Völklinger Str. 49,
40221 Düsseldorf

Telefon 0211-939-0
Telefax 0211-939-4519
poststelle.lka@polizei.nrw.de
www.polizei.nrw.de/lka

Öffentliche Verkehrsmittel:
Straßenbahnlinien 704, 709
Haltestelle: Georg-Schulhoff-Platz
S-Bahnlinien S8, S11, S28
Haltestelle: Völklinger Straße

Zahlungen an:
Landeskasse Düsseldorf
IBAN:
DE 41300500000004100012
BIC :
WELADEDDXXX

Sehr geehrter Herr Sieveke,

für die Gelegenheit zur Darstellung der Sichtweise meiner Behörde im Rahmen des schriftlichen Stellungnahmeverfahrens zum im Betreff angeführten Themenkomplex bedanke ich mich ausdrücklich. Zu den Beschlussvorschlägen nehme ich wie folgt Stellung:

Zu 1. Aufbau eines gesonderten digitalen Kompetenzzentrums

1.1 Ausgangslage

1.1.1 Strafverfolgung/Gefahrenabwehr/Vorfeldinformationen

Im Zusammenhang mit der Beschaffung von Informationen zur Terrorismusbekämpfung sind im Hinblick auf die tatsächlichen

Vorgehensweisen und taktischen Erfordernisse sowie vor dem Hintergrund der unterschiedlichen rechtlichen Rahmenbedingungen drei Zielrichtungen hoheitlichen Handelns zu unterscheiden:

- Maßnahmen, die sich strafverfolgend gegen inkriminierte Veröffentlichungen richten
- Maßnahmen, die auf die gefahrenabwehrende Informationsbeschaffung über potenzielle Anschlagstäter oder Taten gerichtet sind
- Informationsbeschaffungsmaßnahmen, die auf das Erkennen und Beobachten von radikalen Strömungen oder Gruppierungen ohne Hinweise auf eine konkrete Gefährlichkeit gerichtet sind.

Letztere fallen in die nachrichtendienstliche Zuständigkeit, während die ersten beiden Tätigkeitsfelder der Zuständigkeit der Polizei unterfallen.

1.1.2 Besonderheit der digitalen Informationsbeschaffung

Die zentrale Besonderheit bei Ermittlungsmaßnahmen im Internet stellt die „Multilokalität“ sowohl der möglichen Bereitstellung, als auch der Kenntnisnahme von Veröffentlichungen dar. Anders als bei einem nicht-digitalen Tat- oder Ereignisort, der einem örtlichen Zuständigkeits-bereich eindeutig zugeordnet werden kann, befindet sich eine Internet-veröffentlichung im virtuellen Raum und kann von verschiedenen Ermittlern an verschiedenen Orten wahrgenommen und bearbeitet werden. Versuche einer Zuständigkeitszuordnung nach physikalischer Lokalisierung, etwa über Standorte von Servern, haben sich in der Vergangenheit nicht bewährt. Serverstandorte haben aufgrund der Architektur von weltweiten Datennetzwerken häufig keinen Bezug zum tatsächlichen Einstellungs- bzw. Zielort. Die Wahrnehmbarkeit an verschiedenen Ausgabegeräten führt zu einer ineffizienten Mehr- oder

Vielfachbearbeitung, falls keine Zuständigkeitsregelung für die Bearbeitung getroffen werden kann.

Daneben ist zu beachten, dass Zitierstrukturen wie „Likes“ oder „Retweets“, aber auch einfache inhaltliche Bezugnahmen das zu betrachtende Nachrichtenaufkommen über das Maß der ursprünglichen Veröffentlichung hinaus verbreiten. Kontroverse Beiträge an anderer Stelle führen abermals zu einem erhöhten Nachrichtenaufkommen, welches vom „Meinungsgegner“ verursacht wird und für die Beurteilung der ursprünglichen Gefährlichkeit nicht erheblich ist.

Diese Gegebenheiten führen dazu, dass die Effektivität der Bearbeitung entsprechender Sachverhalte mit der Größe des Zuständigkeitsbereiches steigt bzw. die Abstimmungsbedarfe innerhalb der zuständigen Organisationseinheit auftreten und dort abgearbeitet werden können. Erfahrungen hierzu existieren insbesondere aus dem Bereich der Online-Anzeigenerstattung. Aufgrund der Möglichkeit, Online-Anzeigen in den Internetauftritten der verschiedenen Landes- sowie der Bundespolizeibehörden erstatten zu können (neben weiteren Input-Kanälen, wie E-Mail-Postfächern oder Kontaktformularen), kommt es hier, insbesondere bei öffentlichkeitswirksamen Vorgängen, zu Anzeigen und Bürgerhinweisen an unterschiedliche Empfänger. (Als Beispiel sei hier die Veröffentlichung eines YouTube-Videos in den Tagen nach Halloween 2015 genannt. Hierin zeigte ein Beschuldigter Kinder, die an seiner Haustür um Süßigkeiten baten. Der Beschuldigte äußerte diesen gegenüber, erst nach dem Aufsagen des islamischen Glaubensbekenntnisses Süßigkeiten verteilen zu wollen. Dies kommentierte er damit, dass durch das Aufsagen des Glaubensbekenntnisses die Konvertierung zum Islam erfolge und er die Kinder so zu Muslimen gemacht habe. Das Video erregte in den sozialen Netzwerken große Aufmerksamkeit. Aufgrund der weiten

Verbreitung wurde eine hohe zweistellige Anzahl von Online-Anzeigen hierzu erstattet. Diese Anzeigen mussten zur Vermeidung von Mehrfachbearbeitungen in einer Zuständigkeit zusammen geführt werden.)

Die Ansiedlung einer mit der digitalen Informationsbeschaffung befassten Stelle ist aus funktioneller Sicht daher auf einer möglichst hohen organisatorischen Ebene wünschenswert. Daneben sollten in ihr zumindest strafverfolgende und gefahrenabwehrende Zuständigkeiten gebündelt sein. Die Einbindung einer Auswertestelle mit Vorfeld-zuständigkeit ist ebenfalls naheliegend, da so Grenzfälle entweder übergeben oder arbeitsteilig, gemäß der jeweiligen Zuständigkeit, abgearbeitet werden können. Bei unmittelbarer Einbindung einer Behörde mit nachrichtendienstlicher Zuständigkeit entfällt eine andernfalls erforderliche Schnittstelle.

1.2 Vorhandene Strukturen GTAZ und GIZ, GAR und KIA, EUROPOL und ECTC

1.2.1 Gemeinsames Terrorismusabwehrzentrum (GTAZ)

Die vorstehend zusammengefasst dargestellten Erwägungen zur Erforderlichkeit von Zentralität und Kompetenzbündelung haben zur Einrichtung verschiedener Zentren auf Bundesebene geführt, über die eine bundesweite Koordinierung von Maßnahmen der Terrorismusabwehr sowohl in digitalen wie in nicht-digitalen Lebenswelten erfolgt. Aufgrund der historischen Ausgangslage nach den Anschlägen vom 11.09.2001 wurde zunächst im Jahre 2004 das „Gemeinsame Terrorismusabwehrzentrum“ (GTAZ) entwickelt. Die Einrichtung des GTAZ erfolgte vor dem Hintergrund einer verstärkten Bedrohung durch den islamistischen Terrorismus. Dabei handelt es sich um die erste bundesweite Kooperations- und Kommunikationsplattform

zur Sicherstellung eines optimalen Informationsflusses zwischen den handelnden Behörden.

In den Räumen des GTAZ in Berlin kooperieren die ständigen Vertreter der folgenden, insgesamt 40 Behörden:

- Bundesamt für Verfassungsschutz
- Bundeskriminalamt
- Bundesnachrichtendienst
- Generalbundesanwalt
- Bundespolizei
- Zollkriminalamt
- Bundesamt für Migration und Flüchtlinge
- Militärischer Abschirmdienst
- Landesämter für Verfassungsschutz aller 16 Länder
- Landeskriminalämter aller 16 Länder

Die entsandten Vertreter stellen den Informationstransfer zwischen der eigenen Behörde und den übrigen Behördenvertretern im GTAZ sicher.

Die Zusammenarbeitsstrukturen im GTAZ haben sich bewährt, da die Kooperationspartner im Rahmen der Wahrnehmung eigener Zuständigkeiten einen umfassenden bundesweiten behörden-übergreifenden Informationsfluss gewährleisten. Wesentlich für den Erfolg des GTAZ ist die Kooperation zwischen nachrichtendienstlichen und polizeilichen Institutionen und Akteuren. Rechtliche Voraussetzung für deren Kooperation in einem gemeinsamen Zentrum ist die Arbeit in getrennten Strukturen, nämlich in Form der Nachrichtendienstlichen und der Polizeilichen Informations- und Analysestelle (NIAS und PIAS). NIAS- und PIAS-Mitglieder arbeiten in verschiedenen Arbeitsgruppen (AG) eng zusammen, die unterschiedlichen Zwecken dienen: Neben der

aktuellen Fallbearbeitung sowie der Gefahrenprognose werden auch mittel- bzw. längerfristige Analysen erstellt.

Beispiele für vorhandene Arbeitsgruppen sind:

- AG „Tägliche Lagebesprechung“
- AG „Gefährdungsbewertung“
- AG „Operativer Informationsaustausch“
- AG „Fälle/Analysen zum islamistischen Terrorismus“
- AG „Islamistisch-terroristisches Personenpotenzial“
- AG „Deradikalisierung“
- AG „Transnationale Aspekte“
- AG „Statusrechtliche Begleitmaßnahmen“
- Intelligence Board (nur NIAS)

Die verschiedenen Arbeitsgruppen decken die jeweils durch ihre Benennung gekennzeichneten Arbeits- und Zuständigkeitsbereiche ab und gewährleisten damit die Beachtung der unterschiedlichen rechtlichen Rahmenbedingungen für polizeiliches und nachrichtendienstliches Handeln.

Ein wesentliches Werkzeug in der Terrorismusbekämpfung liegt im Miteinander der unterschiedlichen nachrichtendienstlichen und polizeilichen Akteure – ergänzt durch flankierende Maßnahmen im Bereich des Ausländerrechts sowie in einer auf langfristige Wirksamkeit angelegten Abstimmung präventiver und repressiver Erfordernisse (ganzheitlicher Ansatz). Die Stärkung behördenübergreifender Zusammenarbeit sowie die Intensivierung der Kooperation zwischen Vertretern der Strafverfolgungsbehörden schaffen zudem eine „Kultur des Vertrauens“, die unabdingbar ist für die frühzeitige Erkennung und Abwehr von Gefahren. Mehrere Fälle, darunter die erfolgreichen

Ermittlungen im Zusammenhang mit der „Sauerland-Gruppe“, die zur Verhinderung eines Terroranschlags in Deutschland geführt haben, haben gezeigt, dass die Strukturen von PIAS und NIAS im GTAZ funktions- und leistungsfähig sind.

Die Vertreter Nordrhein-Westfalens für die jeweiligen Arbeitsgruppen werden von meiner Behörde in ihrer Funktion als Landeszentralstelle entsandt. Für die Beschaffung der Informationen, die in diesen Arbeitsgruppen ausgetauscht werden, ist auf der Ebene des Landes NRW u. a. die „Zentrale Internet Recherche“ (ZIR) in meiner Behörde zuständig. Eine der Aufgaben der ZIR ist die anlassunabhängige Internetrecherche. Dabei erfasste Gefährdungssachverhalte oder Straftaten werden gegebenenfalls an die zuständige Stelle innerhalb NRWs weitergeleitet, oder, falls eine Zuständigkeit außerhalb NRWs begründet ist, an die zuständige Stelle des jeweils betroffenen Landes weitergeleitet. Die Übergabe des Sachverhalts wird in der zuständigen Arbeitsgruppe begleitet. Durch den Sachvortrag des informierenden Landes erhalten die übrigen Ländervertreter die Möglichkeit, gegebenenfalls vorhandene eigene Erkenntnisse zu ergänzen und weitergehenden Informationsbedarf zu decken.

1.2.2 Gemeinsames Internetzentrum (GIZ)

Die produktiven Erfahrungen in der Zusammenarbeit von Sicherheitsbehörden in der dargestellten Form und die zunehmende Bedeutung des Internets für terroristische Aktivitäten und Radikalisierungen, wie sie auch in der Drucksache 16/10303 beschrieben wird, hat Anfang 2007 zur Einrichtung des „Gemeinsamen Internetzentrums“ (GIZ) zur Beobachtung und Bewertung islamistischer Internetinhalte geführt.

Nach dem Vorbild des GTAZ arbeiten im GIZ Vertreter des

- Bundesamtes für Verfassungsschutz
- Bundeskriminalamtes
- Bundesnachrichtendienstes
- Amtes für den Militärischen Abschirmdienst und
- der Generalbundesanwaltschaft

zusammen. Darüber hinaus steht das GIZ in ständigem Austausch mit den zuständigen Landesbehörden. Die benötigten sprachlichen, technischen und fachlichen Kompetenzen der beteiligten Behörden werden so an einem Ort zusammengeführt, um arbeitsteilig und damit ressourcenschonend vorzugehen. Außerdem wird durch diese Zusammenarbeit eine behördenübergreifend einheitliche Berichterstattung an die zuständigen Entscheidungsträger sichergestellt. Die jeweiligen Ergebnisse werden parallel zu ihrer Behandlung in den jeweiligen Besprechungen („Infoboards“) auf den vorgesehenen Meldewegen, also in der Regel als formalisierter „Informationsaustausch in Staatschutzangelegenheiten“ an die originär zuständige Behörde weitergeleitet. Durch diese parallele Informationsweitergabe wird einem Verlust von Informationen vorgebeugt.

Zusammenfassend stelle ich fest, dass der Kompetenz- und Aufgabenzuschnitt von GTAZ und GIZ in Bezug auf die Beobachtung und Verfolgung islamistischer Bestrebungen nahezu identisch wäre mit demjenigen, der nach hiesigem Verständnis einem neu zu schaffenden „digitalen Kompetenzzentrum“ auf Landesebene gemäß Drucksache 16/10303 zuzuweisen wäre. Weder eine Dezentralisierung der Koordination der Abwehr digitaler Terrorismusgefahren unterhalb der bereits erreichten Strukturen auf Bundesebene, noch den Aufbau von Parallelstrukturen in NRW halte ich, insbesondere vor dem Hintergrund

der unter Nr. 1.2 dargestellten Erwägungen, für sachgerecht oder erforderlich.

1.2.3 Gemeinsamens Abwehrzentrum gegen Rechtsextremismus/ -terrorismus (GAR)

Neben den unter Nr. 1.2 beschriebenen Strukturen stellten die Sicherheitsbehörden nach dem Bekanntwerden des „Nationalsozialistischen Untergrunds“ (NSU) mit dem „Gemeinsamen Abwehrzentrum gegen Rechtsextremismus/-terrorismus“ (GAR) ein vergleichbares Kooperationszentrum zur Bekämpfung der terroristischen Bedrohungen aus dem rechtsextremistischen Spektrum auf. Das GAR ging im Jahr 2012 im dritten, heute noch bestehenden Zentrum, dem „Gemeinsamen Extremismus- und Terrorismusabwehrzentrum“ (GETZ) auf. Neben den Aufgaben der Bekämpfung des Rechtsextremismus/-terrorismus gehören auch die weiteren Phänomenbereiche der Politisch motivierten Kriminalität (PMK), der Linksextremismus, der Ausländerextremismus (ohne Islamismus) sowie weitere nicht zuzuordnende PMK, beispielsweise der militante Tierschutz, zum Aufgabenbereich des GETZ.

Am GETZ sind bisher folgende Behörden beteiligt:

- Bundeskriminalamt
- Bundespolizei
- Europol
- Generalbundesanwalt
- Zollkriminalamt
- Bundesamt für Verfassungsschutz
- Bundesnachrichtendienst
- Militärischer Abschirmdienst
- Bundesamt für Migration und Flüchtlinge

- Bundesamt für Wirtschaft und Ausfuhrkontrolle
- Landesämter für Verfassungsschutz aller 16 Länder
- Landeskriminalämter aller 16 Länder

Besonders hinzuweisen ist hier auf die Beteiligung von Europol, die einen Transfer der Koordinierungsergebnisse auf die europäische Ebene gewährleistet und damit dazu beiträgt, einem Informationsdefizit anderer europäischer Sicherheitsbehörden vorzubeugen.

1.2.4 Koordinierte Internetauswertung (KIA)

Analog zur Aufteilung der Zuständigkeiten zwischen GTAZ und GIZ in digitale und nicht-digitale Lebensräume für den Bereich des Islamismus, findet auch zwischen GETZ und der „Koordinierten Internetauswertung“ (KIA) eine Aufgabenteilung statt. Die Internetauswertung wird hierbei federführend durch das Bundesamt für Verfassungsschutz betrieben, was mit der dortigen Zuständigkeit für die Beschaffung von „Vorfeldinformationen“ korrespondiert.

1.2.5 Europol: European Counter Terrorism Centre (ECTC)

Auf europäischer Ebene arbeitet seit dem 01.01.2016 eine eigens geschaffene Organisationseinheit grenzüberschreitende Sachverhalte mit terroristischen Bezügen auf. Vertreter der nationalen Zentralstellen (für Deutschland das BKA) stellen einen Austausch von Informationen über die Grenzen der Nationalstaaten sicher, sofern diese Informationen einen transnationalen Bezug haben. Rechtliche Fragestellungen zur Voraussetzungen von Datenerhebungen unter dem jeweiligen nationalen Recht und der Weitergabe von Daten an Partnerstaaten gewinnen hier aufgrund der unterschiedlichen nationalen Rechtsetzungen an Bedeutung.

1.2.6 Europäischer Informationsaustausch

Der Vertrag von Prüm bietet seit 2009 einen vereinbarten Rahmen für den europäischen Informationsaustausch zur Verhinderung u. a. von terroristischen Straftaten. Die hierin vereinbarten Rahmenbedingungen sehen innovative Kooperationsformen vor, deren vollständige Umsetzung bisher jedoch nicht erfolgt ist. Eine Erhöhung der Umsetzungsqualität dieser Vereinbarung würde wesentlich größere Erfolgsaussichten bei der Bekämpfung terroristischer Aktivitäten auf europäischer Ebene bieten, als die Schaffung weiterer, paralleler Strukturen. Die Bedeutung des Prümer Vertrages und seiner vollständigen Umsetzung spiegelt sich deutlich in der „Wiesbadener Erklärung“ vom 29./30.09.2015 wider. Darin haben 130 Vertreter nationaler und internationaler Sicherheitsbehörden, darunter auch meiner Behörde, Anforderungen an zukünftige Zusammenarbeitsstandards und Kooperationsformen zur Bekämpfung internationaler Netzwerke der Organisierten Kriminalität und des internationalen Terrorismus formuliert. Angesichts der zunehmend komplexer werdenden Informations- und Kommunikationsstrukturen wird die Notwendigkeit zum Ausdruck gebracht, in den Mitgliedstaaten der EU einheitliche Kommunikationskonzepte und Nutzungskriterien für die unterschiedlichen Kommunikationskanäle zu erstellen und auf EU-Ebene abzustimmen. Eine konsequente Anwendung sowie der Ausbau bereits bestehender Strukturen in der polizeilichen Informationsstruktur (s. auch Nr. 4) ist neuen Projekten vorzuziehen.

Dazu sei angemerkt, dass die Mitglieder der AG Kripo (Arbeitsgemeinschaft der Leiter der Landeskriminalämter und des Bundeskriminalamts) nicht zuletzt auf mein Drängen in der letzten Woche vereinbart haben, die Anwendung SIENA als zentralen Informationskanal für den polizeilichen Informationsaustausch in der EU und den assoziierten Drittstaaten den Ländern zeitnah flächendeckend

zur Verfügung zu stellen. Bislang konnte das System von NRW lediglich im Euregionalen Polizeilichen Informations- und Kooperationszentrum (EPICC) in Heerlen, in dem Polizei NRW mit Vertretern der belgischen und der niederländischen Polizei sowie der Bundespolizei den grenzüberschreitenden Informationsaustausch und die Bearbeitung polizeilicher Rechtshilfeersuchen in der Euregio Maas-Rhein abwickelt, genutzt werden. Künftig soll eine dezentrale Nutzung in allen Kreispolizeibehörden in NRW möglich sein.

Ich füge die „Wiesbadener Erklärung“ als Zusammenfassung der aktuellen Bedarfslage meiner Stellungnahme als Anlage bei.

1.3 Zusammenfassung und Bewertung

Einen Bedarf für ein gesondertes digitales Kompetenzzentrum zur Bekämpfung des internationalen Terrorismus sehe ich aus kriminalfachlicher Sicht nicht. Auf Bundesebene besteht eine leistungsfähige Struktur aus zwei Kompetenzzentren (GTAZ und GETZ), die durch zwei Kompetenzzentren für digitale Lebenswelten ergänzt werden (GIZ und KIA) und die die unterschiedlichen Sicherheitsbehörden zusammenführen. Zu diesen Zentren erfolgt eine Zulieferung relevanter Sachverhalte für NRW unter anderem durch meine Behörde. Sofern eine Verstärkung des Engagements NRWs in der Bekämpfung terroristischer Aktivitäten im Internet beabsichtigt ist, könnte dies meines Erachtens kriminalfachlich zunächst durch eine Verstärkung der auf Landesebene zuliefernden Stelle, also der ZIR, erreicht werden, ohne Verwerfungen in den etablierten Strukturen der Zusammenarbeit zu erzeugen.

Auf aktuelle Mehrbedarfe im digitalen Raum reagiert die Polizei NRW schon heute im Rahmen von phänomenbezogenen Projekten. Nachdem beispielsweise Ende letzten Jahres im Nachgang zum Messerattentat

auf die heutige Kölner Oberbürgermeisterin, Frau Reker, kriminelle Hasskommentare zu ihrer Rolle in der Kölner Flüchtlingsarbeit zunahmen, wurde dieser Entwicklung durch eine Projektgruppe („Taskforce rechte Internethetze“) meiner Behörde in Zusammenarbeit mit der Justiz aufgegriffen. 184 eingeleitete Strafverfahren bis zum 01.03.2016 als Ausfluss dieser Ermittlungstätigkeit belegen die Möglichkeit zur effektiven Reaktion auf kurzfristige Entwicklungen. Auch in diesem Rahmen zeigten sich die oben angesprochenen Abstimmungsnotwendigkeiten mit Sicherheitsbehörden von Bund und Ländern zur Vermeidung von Redundanzen. Diese Abstimmungsfragen strukturell und nachhaltig zu lösen, gehört zum Auftrag einer Bund-Länder-Projektgruppe „Hasspostings“, die unter Beteiligung meiner Behörde ihre Arbeit aufgenommen hat.

Zu 2. Ausübung von Druck auf Anbieter digitaler Kommunikation

Grundsätzlich ist anzumerken, dass es sich bei den bedeutendsten relevanten Akteuren, wie z. B. Facebook oder Google, um international agierende Konzerne handelt, auf die Druck auszuüben auch für das bevölkerungsreichste Land der Bundesrepublik Deutschland nur eingeschränkt möglich ist.

Erfolgversprechender erscheint mir der Ansatz, auf Anbieter zuzugehen, deren Firmensitz in NRW liegt. Hier sehe ich allerdings nicht die Instrumente der klassischen Eingriffsverwaltung als zielführend an. Ein kooperatives Verwaltungshandeln, welches auf die Erreichung einer Selbstverpflichtung, etwa analog zur Freiwilligen Selbstkontrolle im Bereich des Jugendschutzes gerichtet ist, erscheint wirkungsvoller.

In diesem Zusammenhang möchte ich auch auf die Arbeit des Landespräventionsrates hinweisen. Dieser berät unter anderem unter

Beteiligung von Telekommunikationsdienstleistern zu Möglichkeiten der Kriminalitätsvorbeugung. Dem Landespräventionsrat gehören derzeit 36 Mitglieder an, davon 10 Vertreter von Landesministerien und 26 Vertreter sonstiger Institutionen. Durch diese Struktur stellt er eine Brücke zwischen Verwaltung und Zivilgesellschaft dar. Durch die Perspektiverweiterung ist eine Berücksichtigung unterschiedlicher gesellschaftlicher Blickwinkel gewährleistet.

Soweit eine strafrechtliche Relevanz vorliegt, also konkrete terroristische Straftaten oberhalb der Schwelle des § 129 a/b StGB entfaltet bzw. nach § 140 StGB gebilligt werden, besteht mit den gefahrenabwehrenden und strafverfolgenden Eingriffsbefugnissen der Polizei NRW ein ausreichendes Instrumentarium, um Verstöße beweissicher zu verfolgen und die Einhaltung der Rechtsordnung zu gewährleisten. Die Zusammenarbeit mit den Anbietern sozialer Netzwerke unter dem Gesichtspunkt einer bevorrechtigten Markierung problematischer Inhalte durch Sicherheitsbehörden (sogenanntes „Trusted Flagging“) wird derzeit geprüft. Ich beabsichtige, mich an dieser Vorgehensweise zu beteiligen, sobald die Modalitäten abschließend geklärt sind. Bis auf Weiteres wird die allgemein verfügbare „Beitrag melden“-Funktion verwendet.

Zu 3. Schaffung eines rechtlichen Rahmens zur automatischen Übermittlung von Daten an das Kompetenzzentrum

Die Schaffung eines solchen rechtlichen Rahmens, über die bestehenden Vorschriften hinaus, begegnet aus meiner Sicht Bedenken. Die vorgeschlagene Rechtspflicht zur automatischen Datenübertragung käme der Anzeigepflicht des § 138 StGB gleich.

Mit § 138 StGB begründet der Gesetzgeber die Anzeigepflicht für Straftaten oberhalb einer definierten Erheblichkeitsschwelle. In der Fassung nach der Änderung im Jahre 2009 ist nun mit § 138 Abs. 2 Nr. 2 auch die Bildung einer terroristischen Vereinigung von der Vorschrift umfasst. Dieser gesellschaftliche Konsens bildet eine geeignete Trennlinie zwischen anzeigepflichtigen Sachverhalten, deren Nichtanzeige in der Folge strafbewehrt ist und Sachverhalten, deren Anzeige in die moralische Verantwortlichkeit des Einzelnen gestellt ist.

Im Ergebnis befürworte ich eine über den bisherigen Stand hinausgehende Beauftragung zivilgesellschaftlicher Akteure mit polizeilichen Aufgaben nicht.

Zu 4. Einsatz für eine nachhaltige Verbesserung des Informationsflusses von Hinweisen zu terroristischen Aktivitäten zwischen den internationalen Partnern und deren Behörden sowie Kompetenzzentren

Der angesprochene Informationsfluss ist, wie unter 1. bis 3. dargestellt, grundsätzlich leistungsfähig geregelt. Ein Bedarf für eine Veränderung dieser Abläufe ist fachlich nicht erkennbar. Es sind vielmehr Anstrengungen erforderlich, die bestehenden Strukturen noch leistungsfähiger auszugestalten. So sind z. B. für die Informations-austauschverfahren im Rahmen des Prümer Vertrags (s. auch unter Nr. 1.2.6) und des EURODAC-Verfahrens derzeit nur die Abfragen über das Vorliegen von Daten automatisiert möglich (Hit-/No Hit-Verfahren). Um diese Daten auch tatsächlich zu erhalten ist sodann ein traditionelles, mit Zeitverzug verbundenes Rechtshilfeverfahren anzustrengen.

Im Fall des in Recklinghausen in einer Flüchtlingsunterkunft wohnhaften Attentäters des versuchten Anschlags auf ein Polizeirevier in Paris vom 07.01.2016 führte dieses Verfahren dazu, dass Erkenntnisse nur mühsam im Rahmen der Rechtshilfe durch Einzelanfragen in den betreffenden Staaten mit erheblicher zeitlicher Verzögerung recherchiert werden konnten. Im Ergebnis wurde schließlich festgestellt, dass der Täter in sieben europäischen Staaten unter verschiedenen Personalien Asylanträge gestellt und während seines Aufenthaltes in der EU weitere, insgesamt 20 zum Teil ähnliche Identitäten benutzte und unter wechselnden Personalien zahlreiche Straftaten beging.

Hier ist aus meiner Sicht eine unmittelbare Abfragemöglichkeit anzustreben. Die hierzu erforderlichen Vereinbarungen auf europäischer Ebene könnten durch die Landesregierung im Rahmen ihrer Einflussmöglichkeiten befördert werden.

Mit freundlichen Grüßen

Gez. (Jacob)
Direktor Landeskriminalamt NRW

Bundeskriminalamt

Wiesbadener Erklärung

Anlässlich der am 29. und 30. September 2015 im Bundeskriminalamt durchgeführten Fachtagung „Polizeiliche Informationsarchitektur im 21. Jahrhundert in Deutschland und in der Europäischen Union“ diskutierten 130 Expertinnen und Experten nationaler und internationaler Sicherheitsbehörden sowie Vertreter aus der Wissenschaft die vielfältigen Aufgaben und Möglichkeiten im Bereich des Informationsaustausches und gingen dabei auf aktuelle sowie künftige Entwicklungen ein.

Die Teilnehmer waren sich einig, dass internationalen Netzwerken der Organisierten Kriminalität und des internationalen Terrorismus bi- und multilaterale Kooperationsformen[1] und polizeiliche Informationsverbünde[2] entgegenzusetzen sind, die einen raschen und grenzüberschreitenden Informationsaustausch gewährleisten. Bei einem stetigen Anstieg des Informationsaufkommens und knapper werdender Personal-Ressourcen müssen diese unterschiedlichen bi- und multilateralen Kooperationsformen und Informationsverbände strukturiert und effektiv genutzt werden.

In Anbetracht der Komplexität und Dynamik der Entwicklung der Informationsarchitektur wird es zunehmend schwieriger, den polizeilichen Nutzen bzw. den Bezug zum Bedarfsträger herzustellen. Im Laufe der Vorträge und Diskussionen wurde eine teilweise fehlende Konsolidierung und unzureichende Implementierung bestehender Kooperationsformen herausgestellt. So wurden wichtige innovative Kooperationsformen, wie die Prümer Beschlüsse[3], noch nicht konsequent in allen EU-Mitgliedstaaten umgesetzt.

Die im Plenum und in den verschiedenen Panels diskutierten und entwickelten wesentlichen Schlussfolgerungen werden nachfolgend in einer „Wiesbadener Erklärung“ zusammengefasst:

(1) In den Mitgliedstaaten sind einheitliche Kommunikationskonzepte und Nutzungskriterien für die verschiedenen Kommunikationskanäle zu erstellen und auf EU-Ebene abzustimmen.

[1] z.B. Interpol, Europol einschließlich der dortigen Verbindungsbeamten, SIRENE und bilaterale Verbindungsbeamte

[2] Als Beispiele wurden ENFAST (= European Network on Fugitive Active Search) und EURODAC diskutiert; vgl. Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von EURODAC für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens.

[3] Vgl. Beschluss des Rates vom 23.06.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere bei der Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration (2008/615/JI), ABl. 2008 Nr. L 210, S. 1.

(2) In einer polizeilichen Informationsarchitektur in der EU sind statt neuer Projekte und Initiativen bestehende Instrumente und Kooperationsformen anzuwenden, umzusetzen („Konsolidierung vor Neuentwicklung“) und am ganzheitlichen Konzept des European Information Exchange Model (EIXM)[4] auszurichten. Bei der Ausrichtung der Kooperationsformen sind die erkannten Bedarfslagen und Prozesse (national und international) sowie Erfahrungswerte aus der praktischen Anwendung zu berücksichtigen.

(3) Ein international abgestimmtes Verständnis zur gemeinsamen Nutzung bestehender Kooperationsformen muss weiterentwickelt und konsequent umgesetzt werden. Daher ist der Behandlung dieser Themen auf EU-Ebene in politischer[5] und praktischer[6] Hinsicht eine noch stärkere Bedeutung zuzumessen. Dieser Prozess ist auf Basis der EIXM-Empfehlungen u.a. mit Hilfsmitteln wie der „Roadmap on SIENA[7] Implementation“[8] oder der sogenannten „SPOC-Guidelines“[9] voran zu treiben. Auf nationaler und europäischer Ebene sind Geschäftsprozesse zu beschreiben und EU-weit gemeinsame Indikatoren zu entwickeln, welcher Kooperations-Kanal je nach Fallgestaltung geeignet wäre (z.B. für Prüm-Folgeschriftverkehr, Schwedische Initiative, EIS[10]).

(4) SIENA ist als zentraler Kommunikationskanal für den Informationsaustausch in der EU und in den assoziierten Drittstaaten auszubauen. Um den Informationsaustausch zu beschleunigen und Zentralstellen zu entlasten, sind die dezentralen Nutzungsmöglichkeiten von SIENA auszugestalten. Die dezentrale Nutzung von SIENA ist auf nationaler und internationaler Ebene stufenweise und moderat auszubauen, wobei sicherzustellen ist, dass die Informationen für die Auswertung in den Zentralstellen verfügbar sind. Hierfür sind die technischen Anbindungen von SIENA zum jeweiligen nationalen Vorgangsbearbeitungssystem zu erweitern und die Möglichkeiten der automatisierten Datenübertragung und Übersetzungshilfe weiter zu integrieren. Um die hohen rechtlichen und fachlichen Anforderungen des Europol-Kanals auch bei einem erweiterten Nutzerkreis von SIENA einzuhalten, sind die nationalen Prüf- und Bewilligungsbehörden einzubinden (z.B. LKA, IRC[11], SCCOPOL[12]).

---

[4] In der Ende 2012 veröffentlichten Mitteilung zum Europäischen Informationsmodell (EIXM) fordert die EU Kommission eine effektivere Nutzung der bestehenden Informationsstruktur mit konkreten Empfehlungen. Studien belegen, dass diese Empfehlungen bisher von den Mitgliedstaaten nur unzureichend umgesetzt wurden; vgl. Mitteilung der Kommission an das Europäische Parlament und den Rat – Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch vom 07.12.2012. KOM(2012) 735.

[5] z.B. bei der EU-Kommission und dem GS Rat

[6] z.B. in der Ratsarbeitsgruppe Data Protection and Police Information Exchange (DAPIX) und Law Enforcement Working Party (LEWP)

[7] SIENA = Secure Information Exchange Network Application

[8] Um ein staatenübergreifendes gemeinsames Verständnis für die Nutzung von SIENA zu entwickeln und die fachliche Integration in die bestehende Informationsarchitektur zu erleichtern, wurde in einer bei Europol mit MS und Drittpartnern eingerichteten Arbeitsgruppe die Roadmap on SIENA Implementation mit konkreten Zielen und Maßnahmen weiter erarbeitet.

[9] SPOC = Single Point of Contact; die SPOC Guidelines wurden unter Griechischer Präsidentschaft am 20. Februar 2014 erstmals als Entwurf (EU Dokument 6721/14 DAPIX 24) vorgelegt und debattiert.

[10] EIS = Europol Informationssystem

[11] IRC = Internationale Zentren für Rechshilfeersuchen (NL)

[12] SCCOPOL = Section centrale de la coopération opérationnelle de police (FR)

(5) Das in Deutschland gestartete Pilotprojekt des Bundeskriminalamtes mit Baden-Württemberg zur dezentralen Nutzung von SIENA ist für die nationale deutsche Informationsarchitektur, aber auch für andere Mitgliedstaaten von besonderer Bedeutung. Bei einem erfolgreichen Verlauf der Pilotphase ist den Bundesländern eine dezentrale Nutzung von SIENA für einen direkten Informationsaustausch mit Europol und den MS bei nachrichtlicher Beteiligung des BKA als Zentralstelle/ENU[13] anzubieten.

(6) Neben einer technisch und fachlich gründlichen Integration der Kooperationsformen in die bestehenden IT-Systeme ist die Beschulung der Anwender zu intensivieren. Das Training und die Beschulung sollten national (Bund und Länder) und international harmonisiert werden. Insbesondere die Ausweitung der dezentralen Nutzung von SIENA erfordert eine begleitende Ausbildungskonzeption. Neben Qualitätskontrollen sind auch die Übersetzungsleistungen zunehmend dezentral zu erbringen. Daher muss rechtzeitig eine ganzheitliche Ausbildungskonzeption (Bedienung, Recht, Sprache) entwickelt werden, um die Sachbearbeiter auf geeignete und umfassende Weise auf eine Nutzung von SIENA vorzubereiten („SIENA Führerschein“). Bei Weiterentwicklung einer europäischen Informationsvernetzung ist der Bedarf des Anwenders stärker zu berücksichtigen. Die Systeme müssen benutzerfreundlich integriert werden.

(7) Neben den Vorteilen, die eine Erleichterung und Intensivierung des multilateralen Informationsaustausches für eine effektive Bekämpfung der internationalen organisierten Kriminalität bringt, beinhalten die wesentlichen Rechtsgrundlagen für die multilaterale Zusammenarbeit auch neue Anforderungen an den Datenschutz und die IT-Sicherheit. Der Informationsaustausch braucht Schwellen, klare Verantwortlichkeiten, Dokumentation und Kontrolle. Datenschutz und IT-Sicherheit erfordern und benötigen konsistente Konzepte der Informationsarchitektur.

(8) Um einen raschen und grenzüberschreitenden Informationsaustausch zu gewährleisten, ist die bestehende Informationsarchitektur mit einer zunehmenden Automatisierung der Prozesse flexibel und modern weiter zu entwickeln. Vor allem ist die Komplexität der Informationsarchitektur durch eine zunehmende Interoperabilität und Standardisierung bestehender Systeme mit Hilfe von einheitlichen Datenformaten (z.B. UMF[14]) und stabiler Schnittstellen (z.B. X-polizei) auf der Grundlage eines einheitlichen Datenmodells (z.B. IMP[15]) auf europäischer Ebene zu reduzieren. Dabei sollten die Informationsgewinnung und der Informationsaustausch als Gesamtprojekt betrachtet werden.

(9) Bei der Weiterentwicklung von SIENA durch Europol sind auch die besonderen Anforderungen der europäischen Staatsschutzdienststellen zu berücksichtigen, um den Informationsaustausch bei der Bekämpfung des Terrorismus in die Informationsarchitektur besser integrieren zu können.

[13] ENU = Europol National Unit
[14] UMF = Universal Message Format
[15] IMP = Informationsmodell der Polizei

(10) Die „SPOC-Guidelines“ als integraler Bestandteil der „Strategie für das Informationsmanagement im Bereich der inneren Sicherheit in der EU“[16] aus 2009 müssen konsequent umgesetzt werden, um ein flächendeckendes EU-weites 24/7 Monitoring aller wesentlichen Kooperationsrahmen sicher zu stellen.

(11) Die bereits eingerichteten intelligenten und flexiblen Netzwerke (Kompetenzzentren) auf nationaler und internationaler Ebene mit gut ausgebildeten Spezialisten unterschiedlicher Sicherheitsbehörden müssen weiterentwickelt/ausgebaut werden.

(12) Die Zentralstellen in der EU müssen ihre Rolle mit einer dreidimensionalen Aufgabenwahrnehmung weiterentwickeln. Für Deutschland muss neben der Länder-Bund Kooperation gleichermaßen auch die internationale Zusammenarbeit in den Bekämpfungsstrategien mit einfließen. Dabei ist das in Deutschland zurzeit entwickelte PIAV[17] als Beispiel für diese neue dreidimensionale Aufgabenwahrnehmung für das BKA als Zentralstelle unter Beibehaltung der heterogenen IT-Landschaft in den Bundesländern konsequent umzusetzen. Mit Anschluss an das EIS wird PIAV auch perspektivisch Basis für die Informationsversorgung auf europäischer Ebene sein.

(13) Als weiterer Baustein in der Weiterentwicklung einer polizeilichen Informationsarchitektur wird das ADEP[18]-Projekt bewertet. Innerhalb des Projekts ist mit EPRIS[19] ein europäischer Kriminalaktennachweis zu entwickeln, um umgehend feststellen zu können, ob zu einer bestimmten Person innerhalb Europas polizeiliche Informationen vorliegen. Erkenntnisanfragen können so gezielt an den oder die Mitgliedstaaten gestellt werden, in denen polizeiliche Informationen vorliegen. Das EIS und/oder ADEP sind wirkungsvolle Instrumente, um den stetig ansteigenden internationalen Informationsaustausch zu begrenzen, da alle flächendeckenden Erkenntnisanfragen vermieden werden könnten.

(14) Die Frage, ob Europa ein zentrales Informationsmanagement benötigt, das die Elemente der EIMS[20] 2009, Aspekte des Datenschutzes sowie die Aufgaben der neuen Agentur EU-LISA[21] zusammenführt, ist prinzipiell mit „ja“ zu beantworten. In diesem Zusammenhang sollte perspektivisch auch über die Einrichtung/ Bestimmung eines zentralen „EU-Informationsmanagers“ nachgedacht werden.

Europol wird bei der Gestaltung einer europäischen Informationsarchitektur eine zentrale Rolle zugesprochen, um Impulse zu setzen, zu vermitteln und zu koordinieren. Ähnlich wie das Bundeskriminalamt in Deutschland sollte Europol verstärkt als „Information Hub“ und Zentralstelle wirken. Das SIENA-Kommunikationssystems und das EIS werden in diesem Zusammenhang eine Schlüsselfunktion einnehmen

[16] Vgl. Schlussfolgerungen des Rates vom 30.11.2009 (EU Dokument 16637/09 JAI 873).

[17] PIAV = Polizeilicher Informations- und Analyseverbund; mit PIAV werden die bisherigen Meldedienste sowie phänomenbezogene Zentral- und Verbunddateien ersetzt. Die Informationen werden automatisiert in einem Zentralsystem bereitgestellt, aus den Landessystemen angeliefert und bieten deliktsübergreifende Verknüpfungs- und Recherchemöglichkeiten.

[18] ADEP = Automation of the data exchange process

[19] EPRIS = European Police Record Index System

[20] EIMS = European Information Management Strategy

[21] EU-LISA ist die EU-Agentur zum Management von IT-Großsystemen.

Kontakt

Bundeskriminalamt

Internationale Koordinierung

IK 12 – EU- und internationale Zusammenarbeit, Gremien

E-Mail: ik12@bka.bund.de