EUROPÄISCHE
KOMMISSION

Brüssel, den 18.10.2017
COM(2017) 608 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT

Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Elfter Fortschrittsbericht

I. EINFÜHRUNG

Dies ist der elfte Monatsbericht über die Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion. Er beleuchtet die Entwicklungen in zwei der wichtigsten Bereiche: „Bekämpfung des Terrorismus und der organisierten Kriminalität sowie der Instrumente zu ihrer Unterstützung“ und „Stärkung unserer Abwehrbereitschaft und Widerstandsfähigkeit gegen diese Bedrohungen“.

Präsident Juncker betonte in seiner Rede zur Lage der Union[1], dass die Europäische Union aufbauend auf den Fortschritten der vergangenen drei Jahre bei der Terrorbekämpfung stärker werden muss. Wie in der Absichtserklärung[2] an das Europäische Parlament und den Ratsvorsitz sowie in dem ihr beigefügten Fahrplan für eine enger vereinte, stärkere und demokratischere Union angekündigt, legt die Kommission in diesem Bericht ein **Maßnahmenpaket zur Terrorismusbekämpfung** dar, das in den kommenden sechzehn Monaten umgesetzt werden soll. Diese operativen Maßnahmen werden es den Mitgliedstaaten ermöglichen, die durch die jüngsten Terroranschläge zutage getretenen Schwachstellen in Angriff zu nehmen und so die Sicherheit deutlich zu erhöhen. Damit wird ein Beitrag zur Vollendung einer Sicherheitsunion geleistet, in der Terroristen nicht länger Schlupflöcher ausnutzen können, um Gräueltaten zu verüben. Neben diesen kurzfristigen praktischen Maßnahmen arbeitet die Kommission derzeit an einer künftigen Europäischen Aufklärungseinheit, die von Präsident Juncker als Teil seiner Vision für die Europäische Union bis 2025 angekündigt wurde.

Das Antiterrorpaket umfasst:

- Maßnahmen zur Unterstützung der Mitgliedstaaten beim **Schutz des öffentlichen Raums** (Kapitel II), darunter ein Aktionsplan für einen besseren Schutz des öffentlichen Raums und ein Aktionsplan für eine bessere Vorsorge gegenüber Sicherheitsrisiken durch chemische, biologische, radiologische und nukleare Bedrohungen;
- Maßnahmen zur **Unterbindung des Zugangs zu Mitteln, die von Terroristen** für die Planung und Ausführung von Anschlägen **genutzt werden**, etwa **gefährliche Stoffe** oder **Terrorismusfinanzierung** (Kapitel III), einschließlich einer Empfehlung über unmittelbare Maßnahmen, um dem Missbrauch von Ausgangsstoffen für Explosivstoffe vorzubeugen, sowie Maßnahmen zur Unterstützung der Strafverfolgungs- und Justizbehörden, wenn diese in strafrechtlichen Ermittlungen auf **Verschlüsselungsverfahren** stoßen;
- die nächsten Schritte zur **Bekämpfung von Radikalisierung** (Kapitel IV);
- die nächsten Schritte zur Stärkung der **externen Dimension der Terrorismusbekämpfung** (Kapitel V), darunter ein Vorschlag für einen Beschluss des Rates über den Abschluss im Namen der EU des Übereinkommens des Europarats zur Verhütung des Terrorismus sowie des Zusatzprotokolls, und eine Empfehlung an den Rat, die Aufnahme von Verhandlungen über ein überarbeitetes Abkommen über Fluggastdatensätze mit Kanada zu genehmigen.

[1] http://europa.eu/rapid/press-release_SPEECH-17-3165_de.htm.
[2] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_de.pdf.

II. MASSNAHMEN FÜR EINEN BESSEREN SCHUTZ UND EINE GESTEIGERTE WIDERSTANDSFÄHIGKEIT GEGEN TERRORISMUS

1. Besserer Schutz des öffentlichen Raums

Am Beispiel der Anschläge in Barcelona, Berlin, Brüssel, London, Manchester, Paris, Nizza oder auch Stockholm zeigt sich eine Verlagerung des Schwerpunkts in der terroristischen Propaganda und in der Auswahl der Ziele von Terroristen hin zum öffentlichen Raum, etwa zu Fußgängerzonen, Sehenswürdigkeiten, Verkehrsknotenpunkten, Einkaufszentren, Konzertsälen und Plätzen. Was alle diese sogenannten „weichen Ziele" gemein haben, ist ihre Offenheit, ihr öffentlicher Charakter und die Tatsache, dass sich an diesen Orten eine Vielzahl an Menschen ansammelt, weshalb naturgemäß eine Gefährdung besteht.

Wir können mehr tun, um die Anfälligkeit dieser Orte zu verringern, Gefahren frühzeitig zu erkennen und die Widerstandsfähigkeit zu erhöhen. Daher legt die Kommission gemeinsam mit diesem Bericht einen **Aktionsplan für einen besseren Schutz des öffentlichen Raums**[3] vor, der Maßnahmen enthält, um die Mitgliedstaaten auf nationaler, regionaler und lokaler Ebene in ihren Anstrengungen um einen besseren physischen Schutz vor terroristischen Bedrohungen zu unterstützen. Wenngleich das Risiko nie zur Gänze beseitigt werden kann, sollen die Mitgliedstaaten mit dem Aktionsplan dabei unterstützt werden, Gefahren zu erkennen, die Gefährdung öffentlicher Orte zu verringern, die Auswirkungen von Terroranschlägen einzudämmen und die Zusammenarbeit zu verbessern.

Die EU kann den Schutz des öffentlichen Raums auf zwei Arten unterstützen. Zum einen kann sie den **grenzüberschreitenden Austausch bewährter Verfahren unter anderem durch Finanzmittel** fördern. Dazu zählen etwa Förder- und Unterstützungsmaßnahmen für die Entwicklung innovativer und unauffälliger Schutzbarrieren in Städten, die deren offenen Charakter nicht beeinträchtigen („eingebaute Sicherheit"). Die Kommission ergänzt diese Maßnahmen im Aktionsplan durch finanzielle Unterstützung und hat heute über den Fonds für innere Sicherheit – Ausrichtung „Polizei" eine Aufforderung zur Einreichung von Vorschlägen in Höhe von insgesamt 18,5 Mio. EUR veröffentlicht. Diese kurzfristige Finanzierung wird im Jahr 2018 durch eine Finanzierung im Rahmen der Initiative „Innovative Maßnahmen für eine nachhaltige Stadtentwicklung" unter dem Europäischen Fonds für regionale Entwicklung ergänzt, wobei ein Schwerpunkt auf dem Thema „Sicherheit" liegen und die Finanzierung bis zu 100 Mio. EUR betragen wird. Am 15. September 2017 wurde eine öffentliche Konsultation eingeleitet, um Ideen von Städten zu innovativen Lösungen im Bereich Sicherheit zu sammeln. Die Beiträge werden der Kommission als Grundlage für zukünftige Aufforderungen zur Einreichung von Vorschlägen in diesem Bereich dienen.

Zum anderen kann die EU die **Zusammenarbeit mit einem breiten Spektrum von Interessenträgern** vorantreiben, denen im Hinblick auf einen besseren Schutz des öffentlichen Raums eine wesentliche Rolle zukommt. Der Austausch von Erfahrungen und die Bündelung von Ressourcen sollten besser strukturiert werden. Die Kommission wird ein Forum für den Austausch mit privaten Akteuren wie Einkaufszentren, Konzertveranstaltern, Sportstätten, Hotels und Mietwagenfirmen einrichten. Dieses Forum wird dazu beitragen, zu einem gemeinsamen Verständnis aktueller Herausforderungen im Sicherheitsbereich zu

[3] COM(2017) 612 final vom 18.10.2017.

gelangen, und wird öffentlich-private Partnerschaften zur Verbesserung des Schutzes fördern. Auch lokale und regionale Behörden spielen beim Schutz des öffentlichen Raums eine grundlegende Rolle und müssen in entsprechende Tätigkeiten auf EU-Ebene eingebunden werden. Die Kommission wird diese Interessenträger stärker einbeziehen und einen Dialog mit regionalen sowie lokalen Behörden, z. B. Bürgermeistern großer Städte, in die Wege leiten, um Informationen und bewährte Verfahren zum Schutz des öffentlichen Raums auszutauschen. Als Folgemaßnahme zur Erklärung von Nizza[4] vom 29. September 2017 wird die Kommission Anfang nächsten Jahres gemeinsam mit dem Ausschuss der Regionen eine hochrangige Tagung mit den Bürgermeistern, die die Erklärung von Nizza unterzeichnet haben, sowie mit anderen interessierten Vertretern lokaler und regionaler Ebenen organisieren, um den Austausch bewährter Verfahren zum Schutz des öffentlichen Raums fortzusetzen.

Außerdem wird sich die Kommission weiterhin dem Schutz und der Widerstandsfähigkeit **kritischer Infrastrukturen** widmen. Die umfassende Bewertung der EU-Sicherheitspolitik[5] hat unter anderem aufgezeigt, dass das Europäische Programm für den Schutz kritischer Infrastrukturen[6] an neue Bedrohungen angepasst werden muss. Die Kommission hat eine Evaluierung der Richtlinie[7] über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen eingeleitet. In diese Evaluierung werden auch Erfahrungswerte und Entwicklungen der vergangenen Jahre, wie die verabschiedete Richtlinie zur Netz- und Informationssicherheit[8], einfließen. Inzwischen ist das Europäische Programm für den Schutz kritischer Infrastrukturen gestärkt worden, indem neue Herausforderungen wie Bedrohungen durch Insider und hybride Bedrohungen angegangen und die externen Aspekte des Programms durch die Zusammenarbeit mit den angrenzenden Ländern in der östlichen Nachbarschaft und dem westlichen Balkan ausgeweitet wurden.

Der Verkehrssektor ist seit vielen Jahren nicht nur Ziel von Terroranschlägen, sondern eröffnet auch Wege, um Anschläge zu verüben (z. B. Flugzeugentführungen oder Amokfahrten mit LKW). Als Reaktion darauf muss geprüft werden, inwieweit **Sicherheitsvorschriften im Verkehrssektor** für Sicherheit sorgen und gleichzeitig Verkehrsnetze gewährleisten, die einen flüssigen Verkehr ermöglichen. Während der Luftverkehrssektor inzwischen deutlich besser geschützt ist, werden Anschläge immer häufiger entsprechend den sich bietenden Gelegenheiten verübt und zielen verstärkt auf den öffentlichen Raum ab. Dabei ist der **Schienenverkehr** einem hohen Risiko ausgesetzt, da seine Infrastruktur naturgemäß offen ist. Gegenwärtig gibt es keine EU-Rechtsvorschriften,

---

4 Die Erklärung von Nizza wurde auf einer Konferenz der Bürgermeister der Europa-Mittelmeerregion in Nizza am 29. September 2017 verabschiedet, die auf Initiative des Bürgermeisters von Nizza unter Beteiligung der Kommission stattfand, um bewährte Verfahren zur Vorbeugung von Radikalisierung und zum Schutz des öffentlichen Raums zwischen Städten und lokalen sowie regionalen Ebenen auszutauschen. http://www.nice.fr/uploads/media/default/0001/15/TERRORISME%20EUROPE%20Déclaration%20-%20der%20version.pdf.

5 Siehe neunter Bericht über die Fortschritte auf dem Weg zu einer wirksamen und nachhaltigen Sicherheitsunion“ (COM(2017) 407 final vom 26.7.2017) und die beigefügte Arbeitsunterlage der Kommissionsdienststellen (SWD(2017) 278 final).

6 Das Europäische Programm für den Schutz kritischer Infrastrukturen bildet den Rahmen für die Maßnahmen der EU für einen besseren Schutz der kritischen Infrastrukturen in Europa, und zwar in allen Mitgliedstaaten und relevanten Wirtschaftszweigen. Eine wichtige Säule dieser Arbeit ist die Richtlinie über Europäische kritische Infrastrukturen von 2008 (Richtlinie 2008/114/EG vom 8.12.2008).

7 Richtlinie 2008/114/EG vom 8.12.2008.

8 Richtlinie (EU) 2016/1148 vom 6.7.2016.

die den Schienenpersonenverkehr vor Terrorismus und schwerer Kriminalität schützen. Am 15. Juni 2017 startete die Kommission mit den Mitgliedstaaten eine gemeinsame Risikobewertung des Schienenverkehrs, und sie arbeitet an weiteren Maßnahmen zur Erhöhung der Sicherheit im Schienenpersonenverkehr. Darüber hinaus arbeitet die Kommission an einem auf bewährten Verfahren beruhenden Sicherheitsleitfaden für den **gewerblichen Straßenverkehr**. Dabei wird vor allem auf die bessere Sicherung von Lastkraftwagen abgezielt, um das Risiko eines unautorisierten Zugriffs auf LKW, etwa Entführung oder Diebstahl, für terroristische Zwecke einzudämmen. Der Leitfaden soll vor Ende 2017 vorliegen und Empfehlungen für den nationalen Straßenverkehr enthalten. Darüber hinaus wird sich die Kommission auch weiter für mehr **Sicherheit im Seeverkehr** einsetzen, insbesondere für einen besseren Schutz der Seeverkehrsinfrastruktur wie Häfen und Hafeneinrichtungen, Containerschiffe sowie Passagierschiffe (Kreuzfahrtschiffe, Fähren usw.).

2. Bessere Vorsorge gegenüber Sicherheitsrisiken durch chemische, biologische, radiologische und nukleare Bedrohungen

Zwar ist die Wahrscheinlichkeit von Anschlägen mit chemischen, biologischen, radiologischen und nuklearen (CBRN-)Stoffen in der EU nach wie vor gering, doch die Bedrohung durch solche Stoffe entwickelt sich insgesamt weiter. Es gibt Hinweise darauf, dass bestimmte kriminelle Personen oder terroristische Gruppen beabsichtigen könnten, CBRN-Stoffe zu beschaffen, und über das Wissen und die Fähigkeit verfügen, diese für terroristische Zwecke einzusetzen. Auf das Potenzial von Anschlägen mit CBRN-Stoffen wird in terroristischer Propaganda ausführlich eingegangen. Auch die umfassende Bewertung der EU-Sicherheitspolitik[9] hat ergeben, dass es einer besseren Vorsorge vor derartigen Bedrohungen bedarf.

Um die EU in den kommenden Jahren besser gegen die Bedrohung durch CBRN-Stoffe zu wappnen, legt die Kommission mit diesem Bericht einen **Aktionsplan für eine bessere Vorsorge gegenüber Sicherheitsrisiken durch chemische, biologische, radiologische und nukleare Bedrohungen**[10] vor. Er enthält eine Bandbreite von Maßnahmen, um die Vorsorge, die Widerstandsfähigkeit und die Koordinierung auf EU-Ebene zu verbessern, etwa durch die Schaffung eines CBRN-Sicherheitsnetzes der EU, in dem alle einschlägigen Akteure vereint werden sollen. Das Netz wird unter anderem durch ein CBRN-Wissenszentrum ergänzt, das innerhalb des Europäischen Zentrums zur Terrorismusbekämpfung (ECTC) bei Europol eingerichtet werden soll. Da auch die vorhandenen Ressourcen besser genutzt werden müssen, wird in dem Aktionsplan vorgeschlagen, die Vorsorge und Reaktionsfähigkeit durch Schulungen und Übungen mit allen Erstversorgern (aus den Bereichen Strafverfolgung, Zivilschutz und Gesundheit) sowie gegebenenfalls mit Partnern aus dem Militär und der Zivilbevölkerung zu stärken. Ergänzend werden vorhandene Instrumente auf EU-Ebene zum Einsatz kommen, insbesondere das Katastrophenschutzverfahren der Union (UCPM)[11] und die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL). Zur besseren Unterstützung bei größeren CBRN-Vorfällen sollten die Mitgliedstaaten die bestehende Europäische Notfallbewältigungskapazität (EERC) des

---

[9] Siehe neunter Bericht über die Fortschritte auf dem Weg zu einer wirksamen und nachhaltigen Sicherheitsunion“ (COM(2017) 407 final vom 26.7.2017) und die beigefügte Arbeitsunterlage der Kommissionsdienststellen (SWD(2017) 278 final).

[10] COM(2017) 610 final vom 18.10.2017.

[11] Beschluss 1313/2013 vom 17.12.2013.

UCPM, einschließlich des Europäischen Medizinischen Korps, weiter stärken. In diesem Zusammenhang werden die Mitgliedstaaten angehalten, weitere CBRN-Kapazitäten für die EERC bereitzustellen.

Die EU-Vorschriften zu **schwerwiegenden grenzüberschreitenden Gesundheitsgefahren**[12] regeln die Vorsorge und Überwachung sowie die Koordinierung der Reaktion auf gesundheitliche Notfälle innerhalb der EU. In diesem Bereich wird das Frühwarn- und Reaktionssystem der EU besser mit anderen Warnsystemen der EU zu biologischen, chemischen, ökologischen und unbekannten Bedrohungen vernetzt. Im Rahmen des Gesundheitsprogramms werden EU-weite Übungen im Hinblick auf die Notfallvorsorge und -reaktion sowie gemeinsame Maßnahmen zur Unterstützung der Mitgliedstaaten bei der Stärkung von Laboratorien, Impfprogrammen und Kernkapazitäten gemäß den Internationalen Gesundheitsvorschriften finanziert.

Alle diese Initiativen werden durch spezifische Forschungsmaßnahmen, Finanzierungen und die Zusammenarbeit mit einschlägigen internationalen Partnern unterstützt.

III. VORGEHEN GEGEN DIE ZUR UNTERSTÜTZUNG DES TERRORISMUS EINGESETZTEN MITTEL

1. Terrorismusfinanzierung: grenzüberschreitender Zugang zu Finanzinformationen

Informationen über die finanziellen Aktivitäten von Terrorverdächtigen können äußerst wichtige Hinweise für Ermittlungen im Rahmen der Terrorismusbekämpfung liefern. Dank ihrer Zuverlässigkeit und Genauigkeit können Finanzdaten (einschließlich Daten zu Finanztransaktionen) dazu beitragen, Terroristen zu identifizieren, Verbindungen zu Mittätern aufzudecken, Aktivitäten, Logistik und Bewegungen von Verdächtigen zu ermitteln und Terrornetzwerke zu durchschauen. Ein rascher Überblick über die finanziellen Aktivitäten von Verdächtigen und Mittätern kann der Strafverfolgung entscheidende Informationen für die Verhinderung von Anschlägen oder die Ergreifung von Maßnahmen nach Anschlägen bieten. Das wachsende Phänomen kleinerer Anschläge mit einfachsten Mitteln ist mit neuen Herausforderungen verbunden: So ist es bei kurzfristig geplanten Attentaten und Gewaltakten möglicherweise schwieriger, Vorzeichen zu erkennen. Finanztransaktionen im Zusammenhang mit kleineren Anschlägen können zunächst unverdächtig erscheinen, sodass die entsprechenden Informationen den zuständigen Behörden erst nach dem Anschlag zur Kenntnis gebracht werden.

Wie in dem 2016 vorgelegten Aktionsplan zur Bekämpfung der Terrorismusfinanzierung[13] angekündigt, **analysiert die Kommission den Bedarf an zusätzlichen Maßnahmen** mit dem Ziel, den Zugang zu in anderen Hoheitsgebieten der EU verfügbaren Finanzinformationen zum Zweck von Antiterror-Ermittlungen zu erleichtern. Im dritten Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“ vom Dezember 2016[14] hat die Kommission ihre erste Analyse dargelegt und erklärt, sie werde ihre Prüfung fortsetzen und dabei insbesondere mögliche Auswirkungen auf die Grundrechte, vor allem das Recht auf den Schutz personenbezogener Daten, untersuchen. Seither hat die Kommission die Interessenträger konsultiert und die Mechanismen untersucht, über die die

[12] Beschluss 1082/2013/EU vom 22.10.2013.
[13] COM(2016) 50 final vom 2.2.2016.
[14] COM(2016) 831 final vom 21.12.2016.

zuständigen Behörden derzeit auf die betreffenden Informationen – insbesondere auf in anderen Mitgliedstaaten gespeicherte Finanzdaten – zugreifen können; darüber hinaus hat sie ermittelt, welche Hindernisse beim raschen und wirksamen Zugang bestehen, und mögliche Maßnahmen zur Beseitigung dieser Hindernisse genannt.

Neben der laufenden Prüfung wird der **Austausch bewährter Verfahren** bei Ermittlungstechniken und Analysen der Methoden von Terroristen zur Beschaffung und Verschiebung von Geldern weiterhin von der Kommission gefördert, unter anderem durch finanzielle Unterstützung auf der Grundlage einer gerade veröffentlichten Aufforderung zur Einreichung von Vorschlägen im Umfang von 2,5 Mio. EUR.

In diesem Zusammenhang prüft die Kommission auch, wie die **Zusammenarbeit zwischen den zentralen Meldestellen**[15] **verbessert** werden kann, die mit dem Ziel der Verhütung, Aufdeckung und wirksamen Bekämpfung von Geldwäsche und Terrorismusfinanzierung eingerichtet wurden. In einem im Dezember 2016 von den zentralen Meldestellen erstellten Bericht und einer zugehörigen Arbeitsunterlage der Kommissionsdienststellen über die Verbesserung der Zusammenarbeit zwischen den zentralen Meldestellen[16] wird auf eine Reihe von Beschränkungen der inländischen Befugnisse der zentralen Meldestellen eingegangen und ein Lösungsansatz vorgestellt, der Folgendes vorsieht: i) Umsetzung der 4. Geldwäscherichtlinie[17] und ihrer Änderungen[18], über die derzeit verhandelt wird, ii) weitere Initiativen der Plattform der zentralen Meldestellen der EU mit dem Ziel der Vertiefung der operativen Zusammenarbeit, vor allem durch Handlungsempfehlungen, Standardisierungsarbeiten und Geschäftslösungen, die im FIU.NET umzusetzen sind, und iii) Regulierungsmaßnahmen zur Bewältigung anderer Fragen, die sich aus den unterschiedlichen Status und Zuständigkeiten der zentralen Meldestellen ergeben, um vor allem die Koordinierung und den Informationsaustausch sowohl zwischen den zentralen Meldestellen als auch zwischen diesen und den Strafverfolgungsbehörden zu erleichtern.

Darüber hinaus laufen Arbeiten zur Erleichterung des **Zugangs zu Finanzdaten innerhalb der Mitgliedstaaten**. Die vorgeschlagenen Änderungen der 4. Geldwäscherichtlinie[19], über die derzeit mit den gesetzgebenden Organen verhandelt wird, würden dazu führen, dass in allen Mitgliedstaaten zentrale Bank- und Zahlungskontenregister oder elektronische Datenauffindungssysteme eingerichtet würden, die für die zentralen Meldestellen und sonstigen für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zuständigen Behörden zugänglich wären. Nach ihrer Einrichtung in allen Mitgliedstaaten werden diese Register die Ermittlung von Kontodaten erleichtern. Darauf aufbauend bereitet die Kommission eine Initiative zur **Ausweitung des Zugangs der Strafverfolgungsbehörden zu**

---

15 Die zentralen Meldestellen wurden durch den Beschluss 2000/642/JI des Rates vom 17. Oktober 2000 eingerichtet und unterliegen zudem der Richtlinie (EU) 2015/849 vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung. Es handelt sich um operativ unabhängige und autonome Stellen, die dafür zuständig sind, Meldungen über verdächtige Transaktionen und sonstige Informationen, die im Hinblick auf Geldwäsche, damit zusammenhängende Vortaten oder Terrorismusfinanzierung von Belang sind, von einschlägigen Stellen entgegenzunehmen und zu analysieren und die Ergebnisse ihrer Analysen und alle zusätzlichen relevanten Informationen an die zuständigen Behörden weiterzugeben.

16 SWD(2017) 275 final vom 26.6.2017.

17 Richtlinie (EU) 2015/849 vom 20.5.2015.

18 COM(2016) 450 final vom 5.7.2015.

19 COM(2016) 450 final vom 5.7.2016.

diesen Bankkontenregistern[20] vor, um die Kapazitäten der Strafverfolgungsbehörden für die Aufspürung von Bankkonten zu stärken.

Während der Konsultation der Interessenträger wurde außerdem auf **Hindernisse bei der Erlangung von in anderen Mitgliedstaaten verfügbaren Daten zu Finanztransaktionen** hingewiesen. Erforderlichenfalls können Informationen über Bankkonten innerhalb von acht Stunden über die Kanäle der polizeilichen Zusammenarbeit zwischen den Mitgliedstaaten ausgetauscht werden[21]. Der Zugang zu in anderen Mitgliedstaaten verfügbaren Finanztransaktionsdaten kann auch durch die zentralen Meldestellen erleichtert werden. Wenn solche Informationen als Beweismittel in Strafverfahren benötigt werden, müssen sie möglicherweise im Rahmen der gegenseitigen Rechtshilfe angefordert werden. Die Europäische Ermittlungsanordnung[22] bietet neue Möglichkeiten, Finanztransaktionsdaten wesentlich rascher zu erhalten als im Wege der gegenseitigen Rechtshilfe. Einige Monate nach Ablauf der Umsetzungsfrist haben bisher erst 16 Mitgliedstaaten die Europäische Ermittlungsanordnung in ihr Recht umgesetzt. Die übrigen Mitgliedstaaten werden dringend aufgefordert, dies unverzüglich nachzuholen. Die für Anfang 2018 anstehenden Legislativvorschläge zu elektronischen Beweismitteln schließlich werden den grenzüberschreitenden Zugang zu solchen Daten ebenfalls erleichtern.

Die Konsultation der Interessenträger deutet außerdem auf **Hindernisse hin, die die Aufspürung von in anderen Mitgliedstaaten verfügbaren Finanztransaktionsdaten erschweren**. Als erste Maßnahme wird die Kommission hier im Rahmen ihrer laufenden Prüfung die Notwendigkeit, die technische Durchführbarkeit und die Verhältnismäßigkeit miteinander vernetzter zentraler Bankkontenregister untersuchen und dabei sämtliche vorhandenen und geplanten Instrumente zur Erleichterung des Zugangs zu in anderen Mitgliedstaaten verfügbaren Finanztransaktionsdaten berücksichtigen.

Zu diesem Zweck wird die Kommission **weitere Gespräche mit allen betroffenen Interessenträgern** über die Notwendigkeit, technische Durchführbarkeit und Verhältnismäßigkeit möglicher neuer Maßnahmen auf Unionsebene zur Erleichterung und Beschleunigung des grenzüberschreitenden Zugangs zu Finanztransaktionsdaten, einschließlich Verfahren zur Gewährleistung der Vertraulichkeit, führen. Um die laufenden Prüfungen der Verwendung von Finanzinformationen für Ermittlungen im Rahmen der Terrorismusbekämpfung zu bündeln, wird die Kommission im November 2017 ein hochrangiges Treffen der Interessenträger veranstalten. Folgende zentrale Themen werden unter anderem zur Diskussion stehen:

- wichtigste Hindernisse beim wirksamen und zeitnahen Zugang zu in anderen Mitgliedstaaten verfügbaren Finanztransaktionsdaten zum Zweck von Antiterror-Ermittlungen

---

[20] http://ec.europa.eu/info/law/better-regulation/initiatives/Ares-2017-3971182.

[21] Der Rahmenbeschluss 2006/960/JI des Rates (die „schwedische Initiative“) sieht folgende Fristen für die Beantwortung ausländischer Ersuchen durch die Strafverfolgungsbehörden vor: acht Stunden bei dringenden Ersuchen, sofern die erbetenen Informationen oder Erkenntnisse in einer Datenbank verfügbar sind, auf die eine Strafverfolgungsbehörde unmittelbar zugreifen kann, und längere Fristen, wenn die erbetenen Informationen oder Erkenntnisse nicht in einer solchen direkt zugänglichen Datenbank verfügbar sind.

[22] Richtlinie (EU) 2014/41 vom 3.4.2014.

- Notwendigkeit, technische Durchführbarkeit und Verhältnismäßigkeit möglicher neuer Maßnahmen auf Unionsebene zur Erleichterung des grenzüberschreitenden Zugangs zu Finanztransaktionsdaten auf rasche, wirksame und sichere Weise

Die Kommission wird über die Ergebnisse dieser Diskussionen berichten.

2. Explosivstoffe: weitere Beschränkung des Zugangs zu Ausgangsstoffen

Gemäß der **Verordnung über Ausgangsstoffe für Explosivstoffe**[23] sind der Zugang zu und die Nutzung von sieben chemischen Stoffen für die Allgemeinheit beschränkt (in Anhang I der Verordnung aufgeführte „beschränkte Ausgangsstoffe für Explosivstoffe"). Im Februar 2017 nahm die Kommission einen Bericht über die Anwendung der Verordnung durch die Mitgliedstaaten an[24]. Darin gelangte sie zu dem Schluss, dass die Umsetzung der Verordnung zur Verringerung des Zugangs zu gefährlichen Ausgangsstoffen, die für die Selbstherstellung von Explosivstoffen missbraucht werden können, beigetragen hat. Außerdem haben die Mitgliedstaaten Beispielfälle genannt, in denen die Anwendung der Verordnung zu einer frühzeitigen Aufdeckung von Terroranschlägen geführt hat[25]. Um die vollständige Umsetzung der Verordnung sicherzustellen, hat die Kommission im Mai und im September 2016 Vertragsverletzungsverfahren gegen eine Reihe von Mitgliedstaaten eingeleitet, die es versäumt haben, die Verordnung vollständig umzusetzen. Derzeit (Stand Oktober 2017) laufen nur noch zwei Vertragsverletzungsverfahren gegen Spanien und Rumänien.

Trotz dieser gemeinsamen Bemühungen haben die jüngsten terroristischen Anschläge und Vorfälle gezeigt, dass die **Bedrohung durch selbst hergestellte Explosivstoffe** in Europa hoch bleibt. Diese Stoffe sind weiterhin zugänglich und werden für die Selbstherstellung von Explosivstoffen verwendet. Der bei den meisten Anschläge verwendete Explosivstoff war selbst hergestelltes Triacetontriperoxid (TATP), das Berichten zufolge der bevorzugte Explosivstoff von Terroristen ist[26].

Angesichts der derzeitigen Bedrohung durch Ausgangsstoffe für Explosivstoffe ist es erforderlich, sofortige Maßnahmen zu ergreifen, die sicherstellen, dass die genannte Verordnung von allen Mitgliedstaaten möglichst wirksam umgesetzt wird. Daher veröffentlicht die Kommission gemeinsam mit dem vorliegenden Bericht eine **Empfehlung**[27], in der sie Orientierungshilfen für unmittelbare Schritte zur Verhütung des Missbrauchs von Ausgangsstoffen für Explosivstoffe darlegt. Die Kommission ruft die Mitgliedstaaten auf, diese Empfehlung vollumfänglich umzusetzen, um den Zugang zu und die Verwendung von Ausgangsstoffen für Explosivstoffe durch Terroristen so stark wie möglich einzuschränken und zu gewährleisten, dass die Kontrollen der rechtmäßigen Verwendung und die Maßnahmen im Fall verdächtiger Transaktionen verbessert werden. Die Kommission steht bereit, die Mitgliedstaaten dabei zu unterstützen.

---

23 Verordnung (EU) 98/2013 vom 15.1.2013.

24 COM(2017) 103 final vom 28.2.2017.

25 Am 23. Juni 2017 gab das belgische Innenministerium bekannt, es seien innerhalb eines Jahres 30 Meldungen über verdächtige Verkäufe eingegangen. Frankreich hat von Februar bis Juni 2017 11 Meldungen erhalten, die größtenteils Wasserstoffperoxid betrafen.

26 EU-Lage- und Tendenzbericht TE-SAT (EU Terrorism Situation and Trend Report) 2017: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

27 COM(2017) 6950 final vom 18.10.2017.

Darüber hinaus erweitert die Kommission ihre **Überprüfung der Verordnung über Ausgangsstoffe für Explosivstoffe** um eine Evaluierung, gefolgt von einer Folgenabschätzung im ersten Halbjahr 2018. In der Evaluierung sollen die Relevanz, Wirksamkeit, Effizienz, Kohärenz und der Mehrwert der Verordnung untersucht und Probleme und Hindernisse ermittelt werden, die möglicherweise weitere Maßnahmen erfordern werden. In der Folgenabschätzung sollen verschiedene politische Optionen für die Bewältigung der gegebenenfalls ermittelten Probleme und Hindernisse geprüft werden.

3. Verschlüsselung: Unterstützung der Strafverfolgung bei strafrechtlichen Ermittlungen

Die Nutzung der Verschlüsselungstechnik ist von wesentlicher Bedeutung für die Gewährleistung der Cybersicherheit und des Schutzes personenbezogener Daten. In den EU-Rechtsvorschriften wird die Rolle der Verschlüsselung für die Gewährleistung einer angemessenen Sicherheit bei der Verarbeitung personenbezogener Daten besonders hervorgehoben[28]. Gleichzeitig sind die Strafverfolgungs- und Justizbehörden im Rahmen strafrechtlicher Ermittlungen zunehmend mit Herausforderungen konfrontiert, die sich aus der Nutzung von Verschlüsselungstechniken durch Straftäter ergeben. Dadurch werden die Strafverfolgungs- und Justizbehörden in ihrer Fähigkeit beeinträchtigt, die als Beweismittel in strafrechtlichen Ermittlungen benötigten Informationen zu erlangen und Straftäter zu verfolgen und zu verurteilen. Die Nutzung von Verschlüsselungstechniken durch Straftäter und die damit verbundenen Auswirkungen auf strafrechtliche Ermittlungen dürften in den kommenden Jahren weiter zunehmen.

Infolge eines Aufrufs des Rates „Justiz und Inneres“ vom Dezember 2016 hat die Kommission **die Rolle der Verschlüsselung in strafrechtlichen Ermittlungen mit den einschlägigen Interessenträgern erörtert**, wobei sowohl technische als auch rechtliche Aspekte thematisiert wurden. Darin einbezogen waren Sachverständige von Europol, Eurojust, das Europäische Justizielle Netz gegen Cyberkriminalität (EJCN), die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), die Agentur der Europäischen Union für Grundrechte (FRA) sowie Strafverfolgungsbehörden, Industrieverbände und zivilgesellschaftliche Organisationen der Mitgliedstaaten. Über die Fortschritte wurde regelmäßig auf Ebene der Ratsarbeitsgruppe berichtet, und ein Workshop mit den Mitgliedstaaten fand am 18. September 2017 statt. Im Verlauf des Gesamtprozesses fanden mehrere Rundtischgespräche mit Industrieverbänden und zivilgesellschaftlichen Organisationen statt.

Auf der Grundlage dieser Gespräche mit den Mitgliedstaaten und Interessenträgern und ihrer Beiträge gelangt die Kommission zu dem Schluss, dass **zur Unterstützung von Strafverfolgungs- und Justizbehörden**, die in strafrechtlichen Ermittlungen mit der Nutzung von Verschlüsselungstechniken durch Straftäter konfrontiert sind, die im Folgenden genannten Maßnahmen umgesetzt werden sollten. Dazu zählen a) rechtliche Maßnahmen zur Erleichterung des Zugangs zu verschlüsseltem Beweismaterial und b) technische Maßnahmen zur Verbesserung der Entschlüsselungsfähigkeiten. Die Kommission wird die Entwicklungen in diesem Bereich weiter beobachten.

[28] Artikel 32 der Verordnung (EU) 2016/679 vom 27.4.2017.

a) Rechtlicher Rahmen für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln

Die Strafverfolgungsbehörden stehen häufig vor der Herausforderung, Zugang zu in einem anderen Land verfügbaren Beweismitteln zu erlangen. Die laufenden legislativen Entwicklungen auf europäischer Ebene können die Strafverfolgungs- und Justizbehörden in ihrer Fähigkeit unterstützen, Zugang zu notwendigen, aber möglicherweise verschlüsselten Informationen zu erhalten, die in einem anderen Mitgliedstaat verfügbar sind. Für wirksame strafrechtliche Ermittlungen und eine wirksame Strafverfolgung ist ein geeigneter Rahmen erforderlich. Zu diesem Zweck wird die Kommission Anfang 2018 Vorschläge vorlegen, die den grenzüberschreitenden Zugang zu **elektronischen Beweismitteln** erleichtern sollen. Parallel dazu führt die Kommission derzeit eine Reihe konkreter Maßnahmen[29] durch, die bei strafrechtlichen Ermittlungen den grenzüberschreitenden Zugang zu elektronischen Beweismitteln verbessern sollen, darunter die Finanzierung von Schulungen für die grenzüberschreitende Zusammenarbeit, die Entwicklung einer elektronischen Plattform für den Informationsaustausch innerhalb der EU und die Standardisierung der von den Mitgliedstaaten bei der justiziellen Zusammenarbeit verwendeten Formulare.

b) Technische Maßnahmen

Abhängig davon, wie Straftäter Verschlüsselungstechniken nutzen, können die Strafverfolgungs-und Justizbehörden in der Lage sein, einige der Daten wiederherzustellen. Einige Mitgliedstaaten haben nationale Dienste eingerichtet, die über Fachwissen im Umgang mit Verschlüsselungstechniken bei strafrechtlichen Ermittlungen verfügen. Die meisten Mitgliedstaaten haben jedoch keinen Zugang zu einem geeigneten Niveau an Fachwissen und technischen Ressourcen. Dadurch stoßen die Strafverfolgungs- und Justizbehörden bei strafrechtlichen Ermittlungen auf erhebliche Herausforderungen, wenn es um den Zugang zu verschlüsselten Informationen geht. Aus diesem Grund schlägt die Kommission eine **Reihe von Maßnahmen zur Unterstützung der Behörden der Mitgliedstaaten** vor, ohne jedoch die Nutzung von Verschlüsselungstechniken zu untersagen, einzuschränken oder zu schwächen.

Zunächst wird die Kommission **Europol** beim weiteren Ausbau seiner Entschlüsselungsfähigkeiten unterstützen. Zu diesem Zweck hat sie bei der Ausarbeitung des EU-Haushaltsplans für 2018 insgesamt 86 zusätzliche Planstellen im Sicherheitsbereich für Europol vorgeschlagen (19 mehr als im Haushaltsplan 2017), um insbesondere das Europäische Zentrum zur Bekämpfung der Cyberkriminalität bei Europol zu stärken. Der Bedarf an zusätzlichen Ressourcen wird geprüft werden und die Kommission wird im nächsten Fortschrittsbericht zur Sicherheitsunion über die dafür verfügbaren Mittel berichten. Künftige technische Entwicklungen sollten auf der Grundlage der Forschungs- und Entwicklungsarbeiten im Rahmen des Programms „Horizont 2020“ und anderer von der EU finanzierter Programme berücksichtigt werden. Maßnahmen, die die Verschlüsselung schwächen oder Auswirkungen auf eine größere oder unabsehbare Anzahl von Menschen haben könnten, werden nicht berücksichtigt.

Zweitens sollte zur Unterstützung der Strafverfolgungs- und Justizbehörden auf nationaler Ebene ein **Netz von Fachwissenszentren** geschaffen werden. Ohne nationale Initiativen

[29] Siehe achter Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“ (COM(2017) 354 final vom 29.6.2016).

ersetzen zu wollen, könnten so Fähigkeiten und Fachwissen auf nationaler Ebene besser weitergegeben werden. Die Mitgliedstaaten werden aufgerufen, Mittel aus nationalen Programmen des „Fonds für die innere Sicherheit – Polizei“ einzusetzen, um nationale Fachwissenszentren einzurichten, auszuweiten oder weiterzuentwickeln. Auf europäischer Ebene wird die Kommission Europol unterstützen, damit es die Funktionen eines Netzknotenpunkts wahrnehmen kann, der die Zusammenarbeit zwischen den nationalen Fachwissenszentren erleichtert.

Drittens sollte den Mitgliedstaaten ein **Instrumentarium an alternativen Ermittlungstechniken** zur Verfügung stehen, um die Entwicklung und den Einsatz von Maßnahmen zur Erlangung von durch Straftäter verschlüsselten Informationen zu erleichtern. Das Netz der Fachwissenszentren sollte zur Entwicklung dieses Instrumentariums beitragen und das EC3 ist am besten in der Lage, ein Verzeichnis der betreffenden Techniken und Instrumente zu erstellen und zu führen. Maßnahmen, die die Verschlüsselung schwächen oder Auswirkungen auf eine größere oder unabsehbare Anzahl von Menschen haben könnten, werden nicht berücksichtigt.

Viertens sollte der **wesentlichen Rolle von Dienstleistungsanbietern und anderen Partnern aus der Industrie** bei der Bereitstellung von Lösungen mit starker Verschlüsselung Aufmerksamkeit gewidmet werden. Angesichts des Bekenntnisses der Kommission zu einer starken Verschlüsselung würde eine bessere und stärker strukturierte Zusammenarbeit zwischen Behörden, Dienstleistungsanbietern und anderen Industriepartnern auf allen Seiten ein besseres Verständnis der bisherigen und künftigen Herausforderungen fördern. Die Kommission wird strukturierte Dialoge mit den Dienstleistungsanbietern und anderen Unternehmen unter dem Dach des EU-Internetforums und des Netzes der Fachwissenszentren sowie gegebenenfalls unter Einbeziehung der Zivilgesellschaft unterstützen.

Fünftens sollten **Schulungsprogramme** für die Strafverfolgungs- und Justizbehörden sicherstellen, dass die zuständigen Bediensteten besser dafür gerüstet sind, an benötigte Informationen, die von Straftätern verschlüsselt wurden, heranzukommen. Um die Aufstellung von Schulungsprogrammen zu unterstützen, beabsichtigt die Kommission, Mittel von 500 000 EUR im Rahmen des Jahresarbeitsprogramms 2018 des „Fonds für die innere Sicherheit – Polizei“ bereitzustellen. Gegebenenfalls wird auf das Fachwissen der Europäischen Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität (ECTEG) zurückgegriffen. Die Kommission wird außerdem Schulungsmaßnahmen der Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) unterstützen und die Mitgliedstaaten werden aufgerufen, für Schulungen Mittel aus nationalen Programmen des „Fonds für die innere Sicherheit – Polizei“ einzusetzen.

Sechstens ist es erforderlich, angesichts der ständigen Weiterentwicklung der Verschlüsselungstechniken, ihrer zunehmenden Nutzung durch Straftäter und ihrer Auswirkungen auf strafrechtliche Ermittlungen eine **fortlaufende Bewertung der technischen und rechtlichen Aspekte** der Rolle der Verschlüsselung in strafrechtlichen Ermittlungen durchzuführen. Die Kommission wird diese wichtigen Arbeiten weiter fortsetzen. Darüber hinaus wird sie die Einrichtung einer Beobachtungsfunktion in Zusammenarbeit mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität bei Europol, dem Europäischen Justiziellen Netz gegen Cyberkriminalität und Eurojust unterstützen.

IV. Bekämpfung der Radikalisierung

1. Hochrangige Expertengruppe zur Radikalisierung

Die jüngsten, vor allem von Einzeltätern verübten Anschläge sowie die Erkenntnis, wie schnell einige Täter radikalisiert wurden, machen nur zu deutlich, wie wichtig es ist, der Radikalisierung vorzubeugen und sie zu bekämpfen. Die Kommission hat eine **hochrangige Expertengruppe zur Radikalisierung** eingesetzt, um – aufbauend auf dem bisher Erreichten – die Anstrengungen zur Prävention und Bekämpfung der Radikalisierung weiter zu forcieren und die Koordination und Kooperation zwischen allen einschlägigen Akteuren zu verbessern[30]. Aufgabe der Gruppe ist die Ausarbeitung von Empfehlungen für weitere Arbeiten auf diesem Gebiet, wobei noch in diesem Jahr ein erster Zwischenbericht vorgelegt werden soll. Im Dezember 2017 wird die Kommission dem Rat „Justiz und Inneres" über die bisherigen Fortschritte Bericht erstatten. Die Gruppe wird sich auch damit befassen, welche Rahmenbedingungen und beispielsweise weiteren Kooperationsstrukturen auf EU-Ebene benötigt werden, um der Radikalisierung die nötigen Kapazitäten und Kompetenzen entgegensetzen zu können. In diesem Zusammenhang wird sich die Gruppe auch mit der Notwendigkeit und dem Mehrwert eines EU-Zentrums für die Radikalisierungsprävention befassen, das von einigen Mitgliedstaaten gefordert wird.

Zu den Schwerpunktthemen der Gruppe gehört auch die **Radikalisierung in Gefängnissen**. Das Hauptaugenmerk liegt derzeit auf der Umsetzung der Schlussfolgerungen des JI-Rates vom 20. November 2015[31] zur Verstärkung des strafrechtlichen Vorgehens gegen Radikalisierung. Die Kommission wird am 27. Februar 2018 eine Konferenz der Interessenträger zum strafrechtlichen Vorgehen gegen Radikalisierung veranstalten, auf der die Ergebnisse der laufenden Projekte bekannt gegeben werden.

Die Kommission wird die Schlussfolgerungen und Empfehlungen der Gruppe im Arbeitsplan der bereits vorhandenen Initiativen berücksichtigen (insbesondere im Rahmen des Exzellenzzentrums des Aufklärungsnetzwerks gegen Radikalisierung) sowie bei der Nutzung und Ausrichtung seiner Gründungsinstrumente (einschließlich des Fonds für die innere Sicherheit, aber auch anderer Fonds in diesem Zusammenhang wie Erasmus+, das Justizprogramm und der Europäische Sozialfonds).

2. Bekämpfung der Online-Radikalisierung

Die Terroristen nutzen nach wie vor das Internet für die Radikalisierung und Rekrutierung sowie für die Vorbereitung von und Anstiftung zu Anschlägen sowie die Verherrlichung ihrer Gräueltaten. Der Europäische Rat[32], die G7[33] und die G20[34] haben jüngst weitere Maßnahmen gefordert, um dieser globalen Herausforderung zu begegnen und haben in diesem Zusammenhang auch an die Verantwortung der Internetbranche erinnert.

---

30 Siehe achter Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion" (COM(2017) 354 final vom 29.7.2017).

31 Schlussfolgerungen des Rates der Europäischen Union und der im Rat vereinigten Mitgliedstaaten vom 20. November 2015 zur Verstärkung des strafrechtlichen Vorgehens gegen zu Terrorismus und gewaltbereitem Extremismus führende Radikalisierung (14382/15).

32 http://www.consilium.europa.eu/de/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.

33 http://www.consilium.europa.eu/de/press/press-releases/2017/05/26-statement-fight-against-terrorism/.

34 http://www.consilium.europa.eu/de/press/press-releases/2017/07/07-g20-counter-terrorism/.

Im Juli 2017 legte das EU-Internetforum einen **Aktionsplan gegen terroristische Online-Inhalte** vor, in dem die Internetbranche aufgefordert wurde, entschiedene Maßnahmen zu ergreifen, Mittel bereitzustellen und die notwendigen technischen Instrumente zu entwickeln, um schädliches Material schnell erkennen und entfernen zu können. In dem Aktionsplan werden unverzügliche Fortschritte in einem großen Spektrum von Bereichen[35] gefordert und ein Mechanismus für die regelmäßige Berichterstattung über die ergriffenen Maßnahmen und die erzielten Ergebnisse festgelegt.

Am 29. September 2017 richtete die Kommission ein Treffen hoher Beamter des EU-Internetforums aus, um eine Bestandsaufnahme der **Umsetzung des Aktionsplans gegen terroristische Online-Inhalte** vorzunehmen. Immer mehr Unternehmen setzen auf die automatische Erkennung, sodass sie das technische Know-how dafür entwickeln konnten, terroristische Inhalte bereits zu dem Zeitpunkt zu erkennen, an dem diese hochgeladen werden. Einige Unternehmen berichteten, dass sie mittlerweile 75 % der Inhalte automatisch erkennen, wobei die endgültige Entscheidung über die Entfernung dieser Inhalte von Mitarbeitern überprüft wird, während andere 95 % der Inhalte mit eigenen Erkennungstools erkennen. Trotz dieser konkreten Fortschritte drängt die Kommission alle Unternehmen, den Einsatz dieser Instrumente zu intensivieren, um die Erkennung zu beschleunigen, die Dauer, die terroristische Inhalte im Internet verbleiben, zu verkürzen und terroristische Propaganda schneller und wirksamer zu entfernen. Um die Verbreitung terroristischer Inhalte über unterschiedlichste Plattformen aufzuhalten, fordert die Kommission zudem die Unternehmen auf, dringend die „Hash-Datenbank“ zu erweitern, damit entfernte terroristische Inhalte nicht wieder neu auf andere Plattformen hochgeladen werden können. Dieses Instrument sollte sowohl inhaltlich (über die derzeit erfassten Videos und Bilder hinaus) als auch im Hinblick auf die Zahl der teilnehmenden Unternehmen erweitert werden.

Die Kommission wird auch weiterhin Organisationen der Zivilgesellschaft dabei unterstützen, positive **Botschaften als Gegennarrative** im Internet zu verbreiten. Am 6. Oktober 2017 veröffentlichte die Kommission eine Aufforderung zur Einreichung von Vorschlägen, in der Konsortien von Akteuren der Zivilgesellschaft 6 Mio. EUR für die Entwicklung und Durchführung solcher Kampagnen zur Verfügung gestellt werden.

Als nächstes wird die Europäische Kommission am 6. Dezember 2017 das **EU-Internetforum auf Ministerebene** einberufen, an dem hochrangige Vertreter der Internetbranche teilnehmen werden, um die Fortschritte zu bewerten und den Weg für künftige Maßnahmen zu ebnen.

Die im Rahmen des EU-Internetforums ergriffenen Maßnahmen gegen terroristische Online-Inhalte sollten im größeren Zusammenhang der Bekämpfung illegaler Inhalte im Internet gesehen werden. Die Maßnahmen wurden durch eine von der Kommission am 28. September 2017 verabschiedete Mitteilung nochmals untermauert, in der **Leitlinien und Grundsätze für Online-Plattformen** festgelegt wurden, um in Zusammenarbeit mit nationalen Behörden, Mitgliedstaaten und anderen einschlägigen Akteuren den Kampf gegen illegale Online-Inhalte[36] zu intensivieren. Ziel der Mitteilung ist es, die Umsetzung bewährter Praktiken für die Vorbeugung, Erkennung und Entfernung illegaler Inhalte sowie für die Sperrung des

[35] COM(2017) 407 final vom 26.7.2017.

[36] Mitteilung zum „Umgang mit illegalen Online-Inhalten – Mehr Verantwortung für Online-Plattformen“ (COM(2017) 555 final vom 28.9.2017).

Zugangs zu solchen Inhalten zu erleichtern und zu intensivieren, damit eine wirksame Entfernung rechtswidriger Inhalte, eine größere Transparenz und der Schutz der Grundrechte im Online-Umfeld sichergestellt werden. Außerdem gibt sie den Plattformen mehr Klarheit über ihre Haftung, wenn sie proaktiv tätig werden, um illegale Inhalte zu erkennen, zu entfernen oder zu sperren. Die Kommission erwartet von den Online-Plattformen, dass sie in den nächsten Monaten – auch im Rahmen einschlägiger Dialoge, die beispielsweise im EU-Internetforum zu Terrorismus und illegaler Online-Hetze geführt werden – zügig tätig werden.

Parallel hierzu wird die Kommission die Fortschritte überwachen und prüfen, ob zusätzliche, möglicherweise legislative Maßnahmen zur Ergänzung des vorhandenen Regelungsrahmens erforderlich sind, um eine zügige und proaktive Erkennung und Entfernung illegaler Online-Inhalte zu gewährleisten. Diese Arbeiten werden bis Mai 2018 abgeschlossen sein.

Normativ betrachtet stärkt der Kommissionsvorschlag[37] für die **Überarbeitung der Richtlinie über audiovisuelle Mediendienste**, der im Mai 2016 vorgelegt wurde, den Kampf gegen Hassreden. Mit ihrer Überarbeitung soll die Richtlinie an den Rahmenbeschluss zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit[38] und an die Grundrechtecharta angeglichen werden. Zudem ist eine Verpflichtung für die Mitgliedstaaten vorgesehen, dafür zu sorgen, dass Videoplattformanbieter angemessene Maßnahmen ergreifen – etwa indem sie Warn- und Meldeverfahren einführen – um alle Bürgerinnen und Bürger vor der Aufstachelung zu Gewalt und Hass zu schützen.

V. EXTERNE DIMENSION DER TERRORISMUSBEKÄMPFUNG

1. Externe Maßnahmen der EU zur Terrorismusbekämpfung

Mit ihren externen Maßnahmen zur Terrorismusbekämpfung leistet die EU einen Beitrag zu dem übergeordneten Ziel der Stärkung der inneren Sicherheit der Union. Daher sollte der strategische und politische Zusammenhang zwischen der inneren und äußeren Sicherheit der EU weiter im Sinne einer wirksamen und bereichsübergreifenden Terrorismusbekämpfung gestärkt werden.

Die Kommission unterstützt ein großes Spektrum externer Maßnahmen zur Erhöhung der Sicherheit. So wurden seit dem 1. Januar 2017 über 2,3 Mrd. EUR für über 600 Projekte zur Verfügung gestellt. Bei einigen Aktivitäten steht die Sicherheit im Vordergrund (d. h. die Maßnahmen sind speziell auf die Bekämpfung der Terrorismusfinanzierung und der Radikalisierung sowie auf Grenzen und Gefängnisse ausgerichtet), andere sind für die Sicherheit relevant (d. h. die Programme befassen sich mit den Ursachen von Unsicherheit und Leid, indem sie dazu beitragen, die Bildung, den Zugang zu natürlichen Ressourcen und zu Energie, die Regierungsführung sowie den Sicherheitssektor zu verbessern und die Zivilgesellschaft zu unterstützen).

Der Rat „Auswärtige Angelegenheiten“ vom 19. Juni 2017 erneuerte die strategische Ausrichtung auf diesen Gebieten in seinen umfassenden **Schlussfolgerungen zum**

[37] COM(2016) 287 final vom 25.5.2016.
[38] Rahmenbeschluss des Rates 2008/913/JI vom 28.11.2008.

auswärtigen Handeln der EU im Bereich Terrorismusbekämpfung[39]. Die Hohe Vertreterin und die Europäische Kommission werden im notwendigen Umfang gemeinsam auf eine erfolgreiche Umsetzung dieser Schlussfolgerungen hinarbeiten. Für eine termingerechte und umfassende Umsetzung der Schlussfolgerungen und die Berichterstattung an den Rat bis Juni 2018 wurde zwischen dem Europäischen Auswärtigen Dienst und der Europäischen Kommission ein gemeinsamer Koordinierungsprozess eingerichtet. Die Schwerpunkte:

- **Stärkung des Netzes von Experten für Terrorismusbekämpfung in den EU-Delegationen**: In die Planung der EU-Unterstützung und in die lokale Koordinierung der Zusammenarbeit einzelner Mitgliedstaaten mit unseren Partnern in der Terrorismusbekämpfung sollten zunehmend Experten für Terrorismusbekämpfung einbezogen werden. Damit sie diesem größeren Aufgabenumfang gerecht werden können, sollte die Ausbildung dieser Experten vor und während ihres Einsatzes verbessert werden, auch werden ihre Mandatsschreiben eine präzisere Aufgabenstellung enthalten. Zudem werden sie sich auf stabilere Kontakte mit den EU-Agenturen für Justiz und Inneres stützen können. Zur Abdeckung aller Schwerpunktbereiche wird das Netz der Experten für Terrorismusbekämpfung[40] auf das Horn von Afrika, Zentralasien und Südostasien ausgeweitet.
- **Stärkung der Zusammenarbeit zwischen der Gemeinsamen Sicherheits- und Verteidigungspolitik und Maßnahmen der EU-Agenturen für Justiz und Inneres** bei der Sammlung, Auswertung und beim Austausch von Informationen sowie bei der Sondierung, wie die Kontakte zwischen militärischen Stellen und den im Bereich der Strafverfolgung tätigen Stellen für die Zwecke der Terrorismusbekämpfung verbessert werden könnten. Um den Daten- und Informationsaustausch zwischen der Gemeinsamen Sicherheits- und Verteidigungspolitik und der Justiz- und Innenpolitik zu stärken, gilt es, die Überarbeitung von Teilen des geltenden Rechtsrahmens voranzutreiben und in ausgewählte Mandate und Operationen der Gemeinsamen Sicherheits- und Verteidigungspolitik Stellen einzubetten, die sich mit Informationen über Kriminalität befassen. Wichtig wird sein, die Kontakte zu den EU-Agenturen für Justiz und Inneres in vorrangigen Drittländern weiter zu vereinfachen und zu stärken, auch indem der Informationsaustausch zwischen EU-Stellen und Nicht-EU-Stellen möglichst verbessert wird.
- **Stärkung der internationalen Zusammenarbeit in der Terrorismusbekämpfung und in der Prävention und Bekämpfung von gewalttätigem Extremismus** mit Partnerländern im westlichen Balkan, im Nahen Osten, in Nordafrika, mit der Türkei, mit den Golfstaaten und mit Ländern in der Sahelzone und am Horn von Afrika; mit wichtigen strategischen Partnern, wie beispielsweise den Vereinigten Staaten, Kanada und Australien; und mit wichtigen regionalen und multilateralen Partnern wie den Vereinten Nationen, der NATO, dem Globalen Forum „Terrorismusbekämpfung“, der Financial Action Task Force, der Afrikanischen Union, dem Verband Südostasiatischer Nationen, dem Golf-Kooperationsrat und der Arabischen Liga.

---

[39] http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/.

[40] Zur Zeit setzt die EU Experten für Terrorismusbekämpfung in folgenden Delegationen ein: Algerien, Bosnien und Herzegowina (mit einem regionalen Mandat für die Staaten des westlichen Balkans), Tschad (Sahel), Irak, Jordanien, Libanon, Libyen (Einsatzort Tunis), Marokko, Nigeria, Pakistan, Saudi-Arabien, Tunesien und Türkei.

2. Übereinkommen des Europarats zur Verhütung des Terrorismus

Zusammen mit diesem Bericht wird die Kommission **Vorschläge**[41] **für Ratsbeschlüsse über den Abschluss des Übereinkommens des Europarats zur Verhütung des Terrorismus und seiner Zusatzprotokolle** vorlegen, um die internationale Zusammenarbeit in der Terrorismusbekämpfung zu vertiefen. In dem vom Europarat am 16. Mai 2005 verabschiedeten Übereinkommen[42] geht es um die Einstufung terroristischer und mit Terrorismus im Zusammenhang stehender Handlungen als Straftat, um die internationale Zusammenarbeit bei diesen Delikten sowie um den Schutz, die Entschädigung und die Unterstützung von Terrorismusopfern. Das Übereinkommen trat am 1. Juni 2007 in Kraft. Alle EU-Mitgliedstaaten haben das Übereinkommen unterzeichnet, 23 EU-Mitgliedstaaten haben es ratifiziert. Das vom Europarat am 18. Mai 2015 verabschiedete Zusatzprotokoll[43] dient der Ergänzung des Übereinkommens durch Bestimmungen, mit denen die strafrechtlich relevanten Aspekte der Resolution des UN-Sicherheitsrats Nr. 2178 aus dem Jahr 2014[44] über die „Bedrohung des Weltfriedens und der internationalen Sicherheit durch terroristische Handlungen" umgesetzt werden sollen. Das Zusatzprotokoll entspricht dieser Resolution, indem es ein gemeinsames Verständnis der Delikte, die im Zusammenhang mit ausländischen terroristischen Kämpfern stehen, und eine gemeinsame Reaktion auf diese Delikte fördert. Das Zusatzprotokoll trat am 1. Juli 2017 in Kraft.

Die EU unterzeichnete das Übereinkommen und sein Zusatzprotokoll am 22. Oktober 2015. Da die EU ein umfassendes Paket von Rechtsinstrumenten zur Terrorismusbekämpfung verabschiedet hat, darunter die entsprechende Richtlinie[45], ist sie nunmehr bereit, ihrer Zusage nachzukommen und Vertragspartei des Übereinkommens und seines Zusatzprotokolls zu werden.

3. Überarbeitung des Abkommens über Fluggastdatensätze mit Kanada

In seinem Gutachten vom 26. Juli 2017[46] hat der Gerichtshof der EU festgestellt, dass das am 25. Juni 2014 unterzeichnete Abkommen zwischen Kanada und der EU über die Übermittlung und Nutzung von Fluggastdatensätzen nicht in seiner gegenwärtigen Form geschlossen werden kann, da mehrere Bestimmungen nicht mit den von der EU anerkannten Grundrechten, insbesondere nicht mit dem Recht auf Schutz personenbezogener Daten und der Privatsphäre, vereinbar sind. Die Kommission steht jetzt in Kontakt mit Kanada, um auch am Rande des am 19./20. Oktober 2017 in Ischia stattfindenden G7-Ministertreffens die anstehenden Verhandlungen über die Überarbeitung des Abkommens vorzubereiten. Hierzu hat die Kommission dem Rat zusammen mit diesem Bericht **eine Empfehlung**[47] **vorgelegt, die Eröffnung der Verhandlungen zu genehmigen**, in deren Verlauf das Abkommen entsprechend sämtlicher vom Gerichtshof in seinem Gutachten geforderten Nachbesserungen überarbeitet wird. Der Rat wird ersucht, die Eröffnung dieser Verhandlungen zügig zu genehmigen. Da die Verwendung von Fluggastdatensätzen ein wichtiges Instrument zur Bekämpfung terroristischer Straftaten und schwerwiegender grenzübergreifender Kriminalität

41 COM(2017) 606 final vom 18.10.2017 und COM(2017) 607 final vom 18.10.2017.
42 https://rm.coe.int/168008373a.
43 https://rm.coe.int/168047c5ea.
44 http://www.un.org/en/sc/ctc/docs/2015/SCR%202178_2014_EN.pdf.
45 Richtlinie (EU) 2017/541 vom 15.3.2017.
46 Gutachten 1/15 des Gerichtshofs vom 26.7.2017.
47 COM(2017) 605 final vom 18.10.2017.

darstellt, wird die Kommission die erforderlichen Schritte ergreifen, um die Fortsetzung der Fluggastdatenübermittlung an Kanada unter vollständiger Wahrung der Grundrechte im Einklang mit dem Gutachten des Gerichtshofs zu gewährleisten.

In diesem Zusammenhang verweist die Kommission darauf, dass sie die Mitgliedstaaten auch weiterhin bei der Umsetzung der EU-PNR-Richtlinie[48] unterstützen wird. Das Gutachten des Gerichtshofs berührt nicht die Verpflichtungen, die den Mitgliedstaaten aus dieser Richtlinie erwachsen.

4. Stärkung der Zusammenarbeit von Europol mit Drittländern

Wie bereits in den Schlussfolgerungen des Rates „Auswärtige Angelegenheiten" vom Juni 2017 zum auswärtigen Handeln der EU im Bereich Terrorismusbekämpfung [49] und in einschlägigen Regionalstrategien der EU hervorgehoben[50], ist im Kampf gegen Terrorismus und organisierte Kriminalität die Zusammenarbeit mit Drittländern unverzichtbar. Vor Inkrafttreten der neuen Europol-Verordnung[51] am 1. Mai 2017 hatte Europol auf der Grundlage der bis dahin geltenden Rechtsgrundlage[52] mit einigen Drittländern Abkommen über einen Kooperationsrahmen für den Austausch strategischer und technischer Informationen geschlossen. Einige dieser Abkommen sehen auch die Möglichkeit des Austauschs personenbezogener Daten vor[53]. Diese Abkommen bleiben in Kraft.

Seit dem 1. Mai 2017 regelt die neue **Europol-Verordnung** die externen Beziehungen von Europol mit Drittländern, insbesondere die Bedingungen, unter denen personenbezogene Daten mit EU-Stellen, Drittländern und internationalen Organisationen ausgetauscht werden dürfen. Dem Vertrag und der Verordnung zufolge obliegt es der Kommission, im Namen der Union internationale Abkommen mit Drittländern über den Austausch personenbezogener Daten mit Europol auszuhandeln[54]. Soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, kann Europol im Rahmen von Arbeits- und Verwaltungsvereinbarungen Kooperationsbeziehungen mit externen Partnern herstellen und unterhalten, die den Austausch personenbezogener Daten nicht gestatten.

Angesichts des operativen Bedarfs der Union an einer sicherheitspolitischen Zusammenarbeit mit Drittländern und entsprechend der Europol-Verordnung wird die **Kommission dem Rat bis Ende des Jahres Empfehlungen vorlegen**, die Eröffnung von Verhandlungen über

---

48 Richtlinie (EU) 2016/681 vom 27.4.2016.

49 http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/.

50 Hierunter fällt auch die überarbeitete Europäische Nachbarschaftspolitik (JOIN(2015) 50 final vom 18.11.2015).

51 Verordnung (EU) 2016/794 vom 11.5.2016.

52 Beschluss des Rates 2009/371/JI vom 6.4.2009.

53 Europol schloss Abkommen über den Austausch personenbezogener Daten mit folgenden Drittländern: Albanien, Australien, Bosnien und Herzegowina, Kanada, Kolumbien, ehemalige jugoslawische Republik Mazedonien , Georgien, Island, Liechtenstein, Republik Moldau, Monaco, Montenegro, Norwegen, Serbien, Schweiz, Ukraine und Vereinigte Staaten. Der Verwaltungsrat hat die Eröffnung von Verhandlungen über ein Abkommen zwischen Europol und Israel zwar genehmigt, doch die Verhandlungen waren zum Zeitpunkt des Inkrafttretens der neuen Europol-Verordnung noch nicht abgeschlossen.

54 Darüber hinaus sieht die Europol-Verordnung vor, dass für die Übermittlung personenbezogener Daten zwischen Europol und einem Drittland die Kommission einen Beschluss fassen muss, in dem festgestellt wird, dass das betreffende Land ein angemessenes Datenschutzniveau gewährleistet („Angemessenheitsbeschluss").

Abkommen zwischen der EU und Algerien, Ägypten, Israel, Jordanien, Libanon, Marokko, Tunesien und der Türkei zu genehmigen, um die Übermittlung personenbezogener Daten zwischen Europol und diesen Drittländern auf eine Rechtsgrundlage zu stellen[55]. Mit diesen Abkommen wird Europol noch besser in die Lage versetzt, für die Zwecke der Verhütung und Bekämpfung von unter die Ziele von Europol fallenden Straftaten mit diesen Drittländern Kontakte zu pflegen.

VI. SCHLUSSBEMERKUNGEN

In diesem Bericht wird ein Paket von Maßnahmen zur Terrorismusbekämpfung vorgestellt, das die Mitgliedstaaten in ihren Bemühungen um die Abwehr aktueller Sicherheitsbedrohungen weiter unterstützt. Die Kommission legt den Mitgliedstaaten und dem Rat nahe, der Umsetzung dieser Maßnahmen Priorität einzuräumen. Die Kommission wird das Europäische Parlament und den Rat über die erzielten Fortschritte fortlaufend unterrichten.

Der nächste Fortschrittsbericht zur Sicherheitsunion wird im Dezember 2017 vorgelegt und wird insbesondere auf die Interoperabilität der EU-Informationssysteme in den Bereichen Sicherheit, Grenzschutz und Migrationsmanagement eingehen. In diesem Zusammenhang verweist die Kommission nochmals darauf, wie wichtig es ist, bei den Rechtsetzungsprioritäten für diese Informationssysteme Fortschritte zu erzielen.

[55] Abgesehen von den Abkommen mit diesen Drittländern verweist die Kommission auf den strategischen Rahmen für „Angemessenheitsbeschlüsse“ sowie auf andere Instrumente für die Datenübermittlung und die Instrumente für den internationalen Datenschutz, die in der Mitteilung der Kommission über den Austausch und Schutz personenbezogener Daten in einer globalisierten Welt (COM (2017) 7 final vom 10.1.2017) dargelegt werden, in der die Kommission Drittländern nahelegt, dem Europarat-Übereinkommen 108 und dessen Zusatzprotokollen beizutreten.