



Brüssel, den 17.4.2018  
COM(2018) 211 final

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

**Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Vierzehnter  
Fortschrittsbericht**

## I. EINLEITUNG

Dies ist der vierzehnte Bericht 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 der Abwehrbereitschaft und Widerstandsfähigkeit gegen diese Bedrohungen“.

Die brutalen Anschläge in Trèbes und Carcassonne (Frankreich) am 23. März 2018 haben wieder deutlich gemacht, dass die Bedrohung durch Terrorismus in der EU weiterhin hoch ist. Im Rahmen der stetigen Bemühungen in der Sicherheitsunion, diese Bedrohung zu bekämpfen, legte die Kommission zusammen mit diesem Fortschrittsbericht ein neues Sicherheitspaket mit Maßnahmen vor, die das Handlungsfeld von Terroristen und anderen Straftätern einengen und es ihnen erschweren sollen, ihre abscheulichen Handlungen zu planen und auszuführen. Es umfasst Legislativvorschläge zur Verbesserung der grenzüberschreitenden Erfassung von **elektronischen Beweismitteln** und des Zugangs zu **Finanzdaten** zur Untersuchung und Verfolgung, vor allem von schwerwiegenden Straftaten, und zur Stärkung der Zusammenarbeit zwischen den zentralen Meldestellen (*Financial Intelligence Units* – FIU) und den Strafverfolgungsbehörden. Das Paket enthält außerdem operative Maßnahmen, um den Zugang von Terroristen und anderen Straftätern zu eingeführten **Schusswaffen** und **Ausgangsstoffen für Explosivstoffe**, die wie bei einigen der jüngsten Anschläge zur Selbstherstellung von Explosivstoffen missbraucht werden können, zu verhindern. Schließlich wird ein Legislativvorschlag zur Verbesserung der **Sicherheit nationaler Personalausweise und Reisedokumente** es Terroristen und anderen Straftätern erschweren, solche Dokumente zu missbrauchen oder zu fälschen, um in die EU einzureisen oder sich innerhalb der EU zu bewegen.

Der Anschlag in Salisbury am 4. März 2018 war ein schockierendes Beispiel für die echte Bedrohung, die chemische Stoffe für die allgemeine Sicherheit darstellen können. Bei seiner Tagung vom 22. und 23. März 2018 verurteilte der Europäische Rat diesen Anschlag auf das Schärfste. Er betonte, dass die EU als Reaktion hierauf ihre Widerstandsfähigkeit gegen chemische, biologische, radiologische und nukleare Bedrohungen verstärken müsse. In diesem Fortschrittsbericht werden die Maßnahmen beschrieben, die in dieser Hinsicht ergriffen werden und mit denen der Aktionsplan vom Oktober 2017 zur Verbesserung der Abwehrbereitschaft gegen diese Sicherheitsbedrohungen umgesetzt wird. Dieser Fortschrittsbericht informiert auch über den neuesten Stand der Umsetzung anderer Prioritäten der Sicherheitsunion, nämlich Bemühungen zur Bekämpfung der Radikalisierung über das Internet, zur Verbesserung des Informationsaustauschs, zum Schutz des öffentlichen Raums und zur Bekämpfung von Cyberbedrohungen.

## II. EINENGUNG DES HANDLUNGSRAUMS VON TERRORISTEN UND ANDEREN STRAFTÄTERN

### 1. *Neue Instrumente zum Sammeln elektronischer Beweismittel in Strafverfahren*

Elektronische Beweismittel sind in den allermeisten strafrechtlichen Ermittlungen relevant und Justizbehörden müssen immer häufiger Anträge in anderen Zuständigkeitsbereichen stellen, um die notwendigen Beweise von den Diensteanbietern einzuholen. Es ist daher für die Ermittlungen und die Verfolgung von Straftaten, einschließlich Terrorismus und Cyberkriminalität, äußerst wichtig, dass diese Beweise einfacher und schneller grenzübergreifend eingeholt werden können. Zu diesem Zweck hat die Kommission

zusammen mit diesem Fortschrittsbericht zwei Legislativvorschläge zur Verbesserung der grenzüberschreitenden Sammlung elektronischer Beweismittel für Strafverfahren vorgelegt, nämlich einen Vorschlag für eine Verordnung über Europäische Anordnungen zur Herausgabe und Sicherung von elektronischen Beweismitteln in Strafsachen<sup>1</sup> und einen Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Benennung rechtlicher Vertreter zwecks Erhebung von Beweismitteln in Strafverfahren<sup>2</sup>. Die Vorschläge für eine Verordnung und eine Richtlinie werden den zuständigen Strafverfolgungs- und Justizbehörden neue Instrumente an die Hand geben, um elektronische Beweismittel für die Ermittlungen und die Verfolgung von Straftaten, einschließlich Terrorismus und Cyberkriminalität, zu erhalten. Die Kommission reagiert mit diesen Vorschlägen auf die Aufforderungen des Europäischen Parlaments und des Rates, einen EU-Rechtsrahmen für Maßnahmen vorzubringen, um elektronische Beweismittel grenzübergreifend zu sammeln, gleichzeitig aber wirksame Sicherheitsvorkehrungen zum Schutz der Rechte und Freiheiten der Betroffenen vorzusehen<sup>3</sup>.

Die vorgeschlagene Verordnung sieht eine Europäische Erstellungsanordnung und eine Europäische Sicherungsanordnung vor. Mit diesen Anordnungen können die zuständigen Behörden eines Mitgliedstaates direkt von in anderen Mitgliedstaaten ansässigen oder vertretenen Diensteanbietern (Anbieter elektronischer Kommunikationsdienste und spezielle Anbieter von Diensten der Informationsgesellschaft) verlangen, vorhandene elektronische Daten, die in den Anwendungsbereich der Verordnung fallen, für die Ermittlungen und Strafverfolgung auf in dem jeweiligen Fall angemessene und erforderliche Art und Weise zu sichern oder zu erstellen. Damit die Einhaltung dieser Anordnungen sichergestellt ist, werden die Diensteanbieter im Rahmen der vorgeschlagenen Richtlinie verpflichtet, mindestens einen Rechtsvertreter in der Union zu benennen. Angesichts des grenzüberschreitenden Charakters des Internets werden in den Vorschlägen die relevanten Diensteanbieter abgedeckt, die Dienstleistungen in einem oder mehreren Mitgliedstaaten anbieten, ungeachtet des Standorts ihres Hauptsitzes, ihrer Infrastruktur oder des Speicherorts der Daten.

Die vorgeschlagene Verordnung bietet strenge Sicherheitsvorkehrungen zur Sicherstellung der vollständigen Achtung der Grundrechte, wie die vorherige Einschaltung der Justizbehörden und weitere Anforderungen zur Sammlung bestimmter Datenkategorien. Da die Anordnungen nur im Rahmen von strafrechtlichen Verfahren und nur, wenn dies in vergleichbaren nationalen Situationen vorgesehen ist, erteilt werden können, gelten außerdem alle Verfahrensgarantien in Strafsachen. Darüber hinaus enthält die Verordnung spezifische Vorschriften für effektive Rechtsbehelfe für die Betroffenen. Die Verordnung umfasst auch das Recht des Diensteanbieters, in dem ersuchenden Mitgliedstaat oder, wenn die Anordnung zur Vollstreckung übertragen wurde, in dem Aufnahmemitgliedstaat aufgrund festgelegter Gründe eine Prüfung zu verlangen. Hierzu gehören Fälle, in denen es offensichtlich ist, dass die Anordnung nicht von einer zuständigen Behörde ausgestellt oder bestätigt wurde, unvollständig ist, offensichtlich gegen die Charta der Grundrechte der Europäischen Union verstößt oder offensichtlich missbräuchlich ist. Außerdem enthält die Verordnung Mechanismen zur Vermeidung und Minderung potenzieller Konflikte mit Verpflichtungen, die Diensteanbieter möglicherweise nach dem Recht eines Drittlandes zu erfüllen haben.

---

<sup>1</sup> COM(2018) 225 final vom 17.4.2018.

<sup>2</sup> COM(2018) 226 final vom 17.4.2018.

<sup>3</sup> Schlussfolgerungen des Rates zur Verbesserung der Strafjustiz im Cyberspace (ST 9579/16) und Entschließung des Europäischen Parlaments vom 3. Oktober 2017 zur Bekämpfung der Cyberkriminalität (2017/2068 (INI)).

Die Legislativvorschläge stützen sich auf eine gründliche Folgenabschätzung und basieren auf einer zwei Jahre dauernden Konsultation von Fachleuten, Bürgerinnen und Bürgern, Diensteanbietern, Regierungs- und Nichtregierungsorganisationen und Wissenschaftlern.<sup>4</sup> Die Kommission nahm außerdem an entsprechenden Diskussionen im Europarat teil und verfolgte die Entwicklungen in Nicht-EU-Staaten, unter anderem die kürzlich erfolgte Verabschiedung des *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* durch den Kongress der Vereinigten Staaten. Die mit diesem Fortschrittsbericht angenommenen Vorschläge bilden eine Grundlage für einen koordinierten und kohärenten Ansatz, der innerhalb der EU verfolgt wird und von der EU auch auf internationaler Ebene vertreten wird und bei dem die EU-Vorschriften, unter anderem zur Nichtdiskriminierung zwischen EU-Mitgliedstaaten und ihren Staatsangehörigen angemessen berücksichtigt werden. Die Kommission nimmt auch weiter aktiv an den Gesprächen im Rahmen des Übereinkommens des Europarats über Cyberkriminalität teil.

Die Kommission fordert die gesetzgebenden Organe auf, diese Legislativvorschläge, die in der Gemeinsamen Erklärung über die gesetzgeberischen Prioritäten der EU für den Zeitraum 2018-2019 enthalten sind, unverzüglich zu prüfen, um rasch zu einer Einigung zu gelangen.

Parallel zu den Legislativvorschlägen arbeitet die Kommission weiter an **praktischen Maßnahmen zur Verbesserung der justiziellen Zusammenarbeit** auf der Grundlage der Rechtshilfe und der Richtlinie über die Europäische Ermittlungsanordnung<sup>5</sup> sowie der Zusammenarbeit zwischen Behörden und Diensteanbietern innerhalb des bestehenden Rechtsrahmens. Diese Maßnahmen umfassen Schulungen für Behörden, die Förderung des Einsatzes einer einzelnen Kontaktstelle auf nationaler Ebene und die Schaffung einer Online-Plattform für den sicheren Austausch von Anträgen und Antworten auf Europäische Ermittlungsanordnungen, die auf einer elektronischen Version des Formulars für Europäische Ermittlungsanordnungen basieren. Die Kommission arbeitet eng mit den relevanten Agenturen<sup>6</sup> und Interessenvertretern der EU zusammen, um eine rasche Umsetzung zu gewährleisten.

## 2. Vereinfachung des Einsatzes von Finanzdaten zur Prävention, Erkennung, Untersuchung und Verfolgung von schweren Straftaten

Straftäter und Terroristen agieren über verschiedene Mitgliedstaaten hinweg und sind in der Lage, Finanzmittel innerhalb von Stunden zwischen verschiedenen Bankkonten zu transferieren, um ihre Straftaten vorzubereiten oder Erträge aus Straftaten zu verschieben und zu waschen. Ermittlungen bei schwerwiegenden Straftaten und Terrorismus können zum Stillstand kommen, weil kein rechtzeitiger, genauer und umfassender Zugang zu den relevanten Finanzdaten sichergestellt werden konnte.<sup>7</sup> Angesichts der Bedeutung von

---

<sup>4</sup> Der Konsultationsbericht ist abrufbar unter [https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters\\_de](https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_de); weitere Quellen sind abrufbar unter [https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/evidence\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/evidence_en).

<sup>5</sup> Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen (ABl. L 130 vom 1.5.2014, S. 1-36).

<sup>6</sup> Europol, Eurojust und die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL).

<sup>7</sup> Der Europol-Bericht „From suspicion to action: Converting financial intelligence into greater operational impact“ (Vom Verdacht zum Handeln: Umwandlung von Finanzermittlungen in größere operative Maßnahmen), der 2017 veröffentlicht wurde, hebt diese Problematik hervor und betont die Notwendigkeit eines verbesserten Zugangs der Strafverfolgungsbehörden zu Finanzdaten.

Finanzdaten für die Ermittlungen ist es äußerst wichtig, die Zusammenarbeit zwischen den zuständigen Behörden, die für die Bekämpfung von schwerwiegenden Straftaten und Terrorismus zuständig sind, zu verbessern und deren Zugang zu und Nutzung von Finanzdaten im Einklang mit den Grundrechten und den geltenden Verfahrensgarantien zu fördern. Zu diesem Zweck hat die Kommission zusammen mit diesem Fortschrittsbericht einen **Vorschlag für eine Richtlinie zur Vereinfachung des Einsatzes von Finanzdaten und anderer Daten** zur Prävention, Erkennung, Untersuchung und Verfolgung von schweren Straftaten angenommen.<sup>8</sup>

Der Vorschlag, der auf einer gründlichen Folgenabschätzung basiert, ermöglicht bestimmten Strafverfolgungsbehörden und Vermögensabschöpfungsstellen direkten **Zugang zu Bankkontendaten** in einzelstaatlichen zentralen Bankkontenregistern und Kontenabrufsystemen gemäß der Richtlinie zur Bekämpfung der Geldwäsche.<sup>9</sup> Dieser Zugang wird **im Einzelfall zur Bekämpfung von schwerer Kriminalität** gewährt. Hierdurch wird außerdem der Verwaltungsaufwand für Finanzinstitute erheblich reduziert, da sie nicht mehr auf pauschale Datenanfragen von Strafverfolgungsbehörden antworten müssen.

Der Vorschlag verstärkt außerdem die Zusammenarbeit zwischen den nationalen **zentralen Meldestellen** und Strafverfolgungsbehörden sowie zwischen den zentralen Meldestellen in den verschiedenen Mitgliedstaaten. Darüber hinaus werden die Mitgliedstaaten gewährleisten müssen, dass ihre nationalen Europol-Stellen auf Anfragen von Europol nach Daten aus zentralen Bankkontenregistern und nach Finanzdaten und Finanzanalysen antworten. Anfragen von Europol müssen hinreichend begründet werden und im Einzelfall im Rahmen der Zuständigkeit von Europol und der Erfüllung der Aufgaben erfolgen. Ein verbesserter Zugang der Strafverfolgungsbehörden zu Finanzdaten und eine bessere Zusammenarbeit mit den zentralen Meldestellen werden Ermittlungen beschleunigen und die Behörden in die Lage versetzen, grenzüberschreitende Kriminalität effektiver zu bekämpfen. Europol wird auch in die Lage versetzt, die Mitgliedstaaten bei der Verfolgung von Straftaten, die in den Kompetenzbereich von Europol fallen, besser zu unterstützen. Zur Einhaltung der Grundrechte auf den Schutz personenbezogener Daten und Privatsphäre werden in der vorgeschlagenen Richtlinie strenge Sicherheitsvorkehrungen für die Verarbeitung personenbezogener Daten festgelegt.

Die Kommission fordert die gesetzgebenden Organe auf, den Vorschlag, der in der Gemeinsamen Erklärung über die gesetzgeberischen Prioritäten der EU für den Zeitraum 2018-2019 enthalten ist, unverzüglich zu prüfen, um rasch zu einer Einigung zu gelangen. Die Kommission weist außerdem erneut auf die Bedeutung der vollständigen Umsetzung und Anwendung der vierten Richtlinie zur Bekämpfung der Geldwäsche und der von ihr bereitgestellten Instrumente zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung hin. Dies umfasst die Notwendigkeit, den zentralen Meldestellen angemessene Mittel zur Erfüllung ihrer Aufgaben zur Verfügung zu stellen. Darüber hinaus wird im Rahmen der Änderung der vierten Richtlinie zur Bekämpfung der Geldwäsche – die von den gesetzgebenden Organen im Dezember 2017 politisch vereinbart wurde – von der Kommission verlangt, bis Juni 2020 einen Bericht an das Europäische Parlament und den Rat

---

<sup>8</sup> COM(2018) 213 final vom 17.4.2018.

<sup>9</sup> Die gesetzgebenden Organe der Union vereinbarten dies im Dezember 2017 als eine der Änderungen der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission (ABl. L 141 vom 5.6.2015, S. 73).

zu übermitteln, in dem eine mögliche zukünftige Verknüpfung der zentralen Bankkontenregister geprüft wird. Die Kommission führt zu diesem Zweck eine Studie durch und wird ihre Ergebnisse bis Mitte 2019 vorlegen.

### 3. *Strengere Vorschriften für Ausgangsstoffe für Explosivstoffe, die zur Selbsterstellung von Explosivstoffen verwendet werden*

Terroristen und Straftäter verwendeten bei vielen Anschlägen in der EU selbst hergestellte Explosivstoffe, u. a. in Madrid (2004), London (2005), Paris (2015), Brüssel (2016), Manchester (2017) und Parsons Green (2017). Bei einer noch größeren Zahl gescheiterter und vereitelter Anschläge wurde ebenfalls versucht, selbst hergestellte Explosivstoffe einzusetzen. Diese Anschläge zeigen, dass es notwendig ist, den Zugang von Terroristen zu und ihre Nutzung von Ausgangsstoffen für Explosivstoffe, die zur Selbsterstellung von Explosivstoff missbraucht werden können, so weit wie möglich einzuschränken. Zu diesem Zweck hat die Kommission zusammen mit diesem Fortschrittsbericht einen **Vorschlag<sup>10</sup> zur Überarbeitung und Stärkung der bestehenden Einschränkungen in der Verordnung (EU) Nr. 98/2013 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe** verabschiedet.<sup>11</sup> Dies folgt der Empfehlung der Kommission<sup>12</sup> vom Oktober 2017, in der unverzügliche Maßnahmen zur Verhütung des Missbrauchs von Ausgangsstoffen für Explosivstoffe auf der Grundlage bestehender Rechtsvorschriften festgelegt wurden. Der Vorschlag basiert auf einer Reihe von Konsultationen verschiedener Interessenvertretergruppen und einer gründlichen Folgenabschätzung. Nach der Verordnung von 2013 sind die Bereitstellung, die Verbringung, der Besitz und die Verwendung von bestimmten Ausgangsstoffen für Explosivstoffe beschränkt und verdächtige Transaktionen müssen gemeldet werden. Obwohl diese Beschränkungen und Kontrollen zur Senkung der für die Allgemeinheit verfügbaren Mengen von Ausgangsstoffen für Explosivstoffe beigetragen und zu einem Anstieg der gemeldeten verdächtigen Transaktionen geführt haben, haben sie sich als unzureichend zur Vermeidung des Missbrauchs dieser Stoffe durch Terroristen und Straftäter zur Herstellung von Explosivstoffen erwiesen.

Der Vorschlag der Kommission wird helfen, diese Sicherheitslücken zu schließen und den Rechtsrahmen zu stärken und zu klären. Die vorgeschlagene Verordnung (die die frühere Verordnung von 2013 ersetzen wird) wird darauf abzielen, den Zugang der Allgemeinheit zu gefährlichen Ausgangsstoffen für Explosivstoffe durch eine Reihe von Maßnahmen weiter einzuschränken. Es werden zwei zusätzliche Stoffe<sup>13</sup> zur Liste der beschränkten Ausgangsstoffe für Explosivstoffe hinzugefügt, die Möglichkeit, eine Lizenz zu beantragen, wird auf weniger Stoffe beschränkt und die obligatorische Prüfung von Strafregistereinträgen des Antragstellers wird verbessert. Das Registrierungssystem der Verordnung von 2013 wird nicht weitergeführt, da es weniger Sicherheit bietet. Darüber hinaus wird in dem Vorschlag klargestellt, dass die für Wirtschaftsbeteiligte geltenden Vorschriften auch in vollem Umfang für den Online-Verkauf gelten. Die vorgeschlagene Verordnung wird die Durchsetzung durch die zuständigen Behörden und die Übermittlung von Informationen entlang der Lieferkette verbessern. So wird es durch die vorgeschlagene Verordnung erheblich schwieriger für Terroristen, Explosivstoffe selbst herzustellen. Die Kommission fordert die gesetzgebenden

---

<sup>10</sup> COM(2018) 209 final vom 17.4.2018.

<sup>11</sup> Verordnung (EU) Nr. 98/2013 des Europäischen Parlaments und des Rates vom 15. Januar 2013 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe (ABl. L 39 vom 9.2.2013, S. 1-11).

<sup>12</sup> Empfehlung der Kommission vom 18.10.2017 für unverzügliche Maßnahmen zur Verhütung des Missbrauchs von Ausgangsstoffen für Explosivstoffe (C(2017) 6950 final).

<sup>13</sup> Schwefelsäure und Ammoniumnitrat.

Organe auf, den Legislativvorschlag unverzüglich zu prüfen, um rasch zu einer Einigung zu gelangen.

#### 4. *Verbesserte Sicherheit bei Personalausweisen und Aufenthaltsdokumenten zum Verhindern von Dokumentenfälschung und der Verwendung falscher Identitäten*

Wie die Statistik der Europäischen Agentur für die Grenz- und Küstenwache über gefälschte Dokumente zeigt, sind nationale Personalausweise mit schwachen Sicherheitsmerkmalen innerhalb der EU die am häufigsten missbräuchlich verwendeten Reisedokumente. Als Teil der europäischen Reaktion auf die Fälschung von Reisedokumenten im Aktionsplan vom Dezember 2016<sup>14</sup> verabschiedete die Kommission zusammen mit diesem Fortschrittsbericht einen **Vorschlag für eine Verordnung zur Verbesserung der Sicherheit von Personalausweisen, die für Bürgerinnen und Bürger der EU ausgestellt werden und von Aufenthaltsdokumenten, die für Bürgerinnen und Bürger der EU und deren Familien ausgestellt werden.**<sup>15</sup> Im Einklang mit dem Recht auf Freizügigkeit in der EU können EU-Bürgerinnen und -Bürger Personalausweise als Reisedokumente sowohl für Reisen innerhalb der EU als auch beim Grenzübertritt an den Außengrenzen der EU zur Wiedereinreise in die EU verwenden. In bestimmten Fällen können EU-Bürgerinnen und -Bürger mit ihrem Personalausweis in Drittländer einreisen. Aufenthaltsdokumente von Familienmitgliedern aus Nicht-EU-Ländern, die in Verbindung mit einem Reisepass verwendet werden, gewähren dem Inhaber das Recht, ohne Visum in die EU einzureisen, wenn er/sie von einer EU-Bürgerin oder einem EU-Bürger begleitet wird. Die EU-Gesetzgebung sieht bereits Normen für die Sicherheitsmerkmale und biometrischen Daten (Gesichtsbild und Fingerabdrücke) in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten vor.<sup>16</sup>

Durch die Verbesserung der Sicherheitsmerkmale von Personalausweisen und Reisedokumenten wird es Straftätern erschwert, solche Dokumente zu missbrauchen oder zu fälschen, um sich innerhalb der EU zu bewegen oder die Außengrenzen der EU zu überqueren. Sicherere Personalausweise werden zur Stärkung der Verwaltung der EU-Außengrenzen beitragen (auch hinsichtlich der Herausforderung in Bezug auf zurückkehrende terroristische Kämpfer und deren Familienangehörige); gleichzeitig erleichtern es sicherere und zuverlässigere Dokumente den EU-Bürgerinnen und Bürgern, ihr Recht auf Freizügigkeit wahrzunehmen.

Der Vorschlag der Kommission, der auf einer gründlichen Folgenabschätzung und einer öffentlichen Konsultation basiert, legt daher Mindeststandards für die Dokumentensicherheit bei nationalen Personalausweisen fest, wozu insbesondere ein biometrisches Foto und Fingerabdrücke gehören, die in einem Chip im Personalausweis gespeichert werden. In dem Vorschlag sind außerdem Mindestinformationen, die in den ausgestellten Aufenthaltsdokumenten von mobilen EU-Bürgerinnen und -Bürgern enthalten sein müssen, sowie eine vollständige Harmonisierung der Aufenthaltsdokumente von Familienmitgliedern aus Nicht-EU-Ländern vorgesehen.

Die Kommission fordert die gesetzgebenden Organe auf, den Legislativvorschlag unverzüglich zu prüfen, um rasch zu einer Einigung zu gelangen.

---

<sup>14</sup> COM(2016) 790 final vom 8.12.2016.

<sup>15</sup> COM(2018) 212 final vom 17.4.2018.

<sup>16</sup> Verordnung (EG) Nr. 2252/2004 (ABl. L 385 vom 29.12.2004, S.1).

## 5. *Verbesserte Kontrollen der Ein- und Ausfuhr von Schusswaffen zur Bekämpfung des illegalen Waffenhandels*

Die Kommission hat eine Reihe von Maßnahmen ergriffen, um die Lieferung von Schusswaffen an Straftäter und Terroristen einzuschränken. Zur Ergänzung der Maßnahmen gegen illegalen Waffenhandel<sup>17</sup> und der im Mai 2017 überarbeiteten Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen, verabschiedete die Kommission zusammen mit dem vorliegenden Fortschrittsbericht eine **Empfehlung**<sup>18</sup> über Sofortmaßnahmen zur Verbesserung der Sicherheit bei der Ausfuhr, Einfuhr und Durchfuhr von Feuerwaffen, deren Teilen und wesentlichen Komponenten und Munition. Mit der Empfehlung werden die EU-Mitgliedstaaten aufgefordert, Maßnahmen zu ergreifen, um **die Verfolgbarkeit und Sicherheit der Ausfuhr- und Einfuhrkontrollverfahren für Feuerwaffen und die Zusammenarbeit zwischen den Behörden bei der Bekämpfung des illegalen Handels mit Feuerwaffen zu verbessern**. Diese Empfehlung folgt dem Bericht der Kommission vom Dezember 2017 über die Durchführung der Verordnung (EU) Nr. 258/2012<sup>19</sup> über die Aus- und Einfuhr von Schusswaffen. In dem Bericht wird geschlussfolgert, dass es notwendig ist, das System der Ausfuhr- und Einfuhrgenehmigungen für Schusswaffen zu stärken, um die Bedingungen für den legalen Handel zu überwachen und so besser gegen den illegalen Waffenhandel kämpfen zu können. Die Kommission wird das Ergebnis dieser Empfehlung, das in die Gesamtüberwachung der Durchführung der Verordnung (EU) Nr. 258/2012 einfließen wird, überwachen.

### III. ANDERE PRIORITÄTEN IM BEREICH DER SICHERHEIT

#### 1. *Bekämpfung terroristischer Inhalte im Internet*

Wie im Arbeitsprogramm der Kommission für 2018 und in früheren Fortschrittsberichten zur Sicherheitsunion dargelegt, fördert und verstärkt die Kommission die Zusammenarbeit mit Internetplattformen bei der Erkennung und Entfernung terroristischer und sonstiger illegaler Inhalte im Internet. Am 1. März 2018 unternahm die Kommission einen weiteren wichtigen Schritt zur Bewältigung des dringenden und schwerwiegenden Problems terroristischer Inhalte im Internet mit der Annahme einer **Empfehlung für** wirksame Maßnahmen, die von Anbietern von Online-Diensten und Mitgliedstaaten zu treffen sind, um die Bemühungen gegen **illegale Online-Inhalte, einschließlich terroristischer Inhalte**, zu verstärken.<sup>20</sup>

Aufbauend auf der Mitteilung der Kommission von September 2017 zum Umgang mit illegalen Online-Inhalten<sup>21</sup> werden mit der Empfehlung Anbieter von Online-Diensten nachdrücklich dazu aufgefordert, eine schnellere Erkennung und Entfernung von illegalen Online-Inhalten sicherzustellen, die Zusammenarbeit zwischen Anbietern von Online-Diensten, vertrauenswürdigen Hinweisgebern und EU-Strafverfolgungsbehörden zu

---

<sup>17</sup> Siehe den EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen und Explosivstoffen und deren unerlaubte Verwendung (COM(2015) 624 final vom 2.12.2015). Die Zerschlagung von organisierten Verbrecherbanden, die in den unerlaubten Handel, die unerlaubte Verbreitung und die unerlaubte Verwendung von Feuerwaffen verwickelt sind, ist auch eine Priorität im EU-Politikzyklus für organisierte und schwere internationale Kriminalität für den Zeitraum 2018-2021.

<sup>18</sup> C(2018) 2197.

<sup>19</sup> Verordnung Nr. 258/2012 zur Einführung von Ausfuhrgenehmigungen für Feuerwaffen, deren Teile, Komponenten und Munition sowie von Maßnahmen betreffend deren Einfuhr und Durchfuhr.

<sup>20</sup> Empfehlung der Kommission vom 1.3.2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten (C(2018) 1177 final).

<sup>21</sup> Mitteilung der Kommission – Umgang mit illegalen Online-Inhalten – Mehr Verantwortung für Online-Plattformen, COM(2017) 555 final vom 28.9.2017.



verstärken, die Transparenz der Meldungen an Behörden zu erhöhen und Sicherheitsvorkehrungen für die Grundrechte der Bürgerinnen und Bürger zu gewährleisten. Die Empfehlung bietet eine praktische Orientierungshilfe für Anbieter von Online-Diensten, um terroristische Inhalte schneller aus dem Netz zu nehmen und besser mit den Strafverfolgungsbehörden zusammenzuarbeiten. Da terroristische Inhalte üblicherweise in der ersten Stunde nach ihrem Erscheinen im Internet am gefährlichsten sind und angesichts der spezifischen Erfahrungen und Verantwortlichkeiten der zuständigen Behörden und Europol, wird in der Empfehlung betont, dass im Allgemeinen in Verweisen gefundene Inhalte von den Anbietern von Online-Diensten geprüft und gegebenenfalls innerhalb einer Stunde entfernt werden müssen beziehungsweise der Zugang gesperrt werden sollte. Plattformen wird außerdem empfohlen, proaktiv zu sein und automatische Instrumente zur Erkennung und Ermittlung von terroristischen Inhalten zu nutzen; sie werden aufgefordert, verfügbare technologische Instrumente zu nutzen, um sicherzustellen, dass solche Inhalte nicht erneut auf andere Plattformen hochgeladen werden.

Derzeit wird ein Bericht erstellt, um eine Überwachung der Auswirkungen dieser Empfehlung zu ermöglichen. Die Informationen, die von Anbietern von Online-Diensten bis Anfang Mai 2018 erwartet werden, werden der Kommission helfen zu entscheiden, ob der gegenwärtige Ansatz ausreicht oder ob zusätzliche Maßnahmen erforderlich sind, um illegale Online-Inhalte rasch und proaktiv zu erkennen und zu entfernen, einschließlich möglicher Legislativmaßnahmen zur Ergänzung des bestehenden Rechtsrahmens.

## 2. *Interoperabilität von Informationssystemen und verbesserter Datenaustausch*

Mit ihrer Arbeit an verbesserten und intelligenteren Informationssystemen in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung geht die EU Mängel im Informationsmanagement und in der Weitergabe von Daten so schnell wie möglich und als oberste Priorität an. Alle damit verbundenen Legislativvorschläge sind in der Gemeinsamen Erklärung über die gesetzgeberischen Prioritäten der EU für den Zeitraum 2018-2019 enthalten. Die Gespräche zwischen den gesetzgebenden Organen über die Legislativvorschläge zur **Interoperabilität** der EU-Informationssysteme schreiten voran. Nach der Tagung des Rates (Justiz und Inneres) am 8. März 2018, bei der die Mitgliedstaaten ihre breite Unterstützung für die von der Kommission vorgeschlagenen Interoperabilitätskomponenten ausgesprochen haben, möchte der Rat bis Juni 2018 einen allgemeinen Ansatz beschließen. Die Gespräche über technische Aspekte im Europäischen Parlament gehen auch voran und sollen bis Juli 2018 in einem Trilog mit den gesetzgebenden Organen fortgeführt werden; noch vor Ende des Jahres soll eine Einigung erzielt werden. Dafür – und wie im Dezember 2017 angekündigt<sup>22</sup> – ist es erforderlich, relevante Änderungen an den Interoperabilitätsvorschlägen für diejenigen Rechtsinstrumente<sup>23</sup>, die derzeit von den gesetzgebenden Organen verhandelt werden, vorzulegen. Da alle das Ziel verfolgen, sich noch vor Ende des Jahres 2018 über die Interoperabilitätsvorschläge zu einigen, wie in der Gemeinsamen Erklärung über die gesetzgeberischen Prioritäten der EU für den Zeitraum 2018-19 festgelegt, **muss wiederum rasch eine Einigung über die Dokumente erreicht werden, die derzeit noch verhandelt werden.** In jedem Fall wird die Kommission

---

<sup>22</sup> Siehe „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“ – Zwölfter Fortschrittsbericht (COM(2017) 779 final vom 12.12.2017).

<sup>23</sup> Die vorgeschlagenen Verordnungen über das Europäische Reiseinformations- und -genehmigungssystem, das Europäische Strafregisterinformationssystem für Drittstaatsangehörige, Eurodac, das Schengener Informationssystem und eu-LISA.

bis Mitte Juni 2018 alle erforderlichen Änderungen an ihren Interoperabilitätsvorschlägen vorlegen, sodass die Trilog ab Juli 2018 beginnen können.

Die interinstitutionellen Verhandlungen über ein **Europäisches Reiseinformations- und -genehmigungssystem** (ETIAS) befinden sich in der Endphase und die Annahme sollte in den kommenden Wochen erfolgen.

Es wird intensiv daran gearbeitet, den Trilog zwischen den gesetzgebenden Organen über die drei Legislativvorschläge zur Stärkung des **Schengener Informationssystems** (SIS) voranzutreiben, um zu einer politischen Einigung zu gelangen. Die Kommission fordert die gesetzgebenden Organe auf, bis Ende Mai 2018 zu einer Einigung zu gelangen. Parallel zu dieser gesetzgeberischen Tätigkeit wurde das **automatisierte Fingerabdruck-Identifizierungssystem** (AFIS) am 5. März 2018 zur Stärkung des Schengener Informationssystems in seiner derzeitigen Form eingeführt. Diese technische Neuerung bedeutet eine unmittelbare und signifikante Verbesserung der Arbeit der Grenzschutzbeamten und Strafverfolgungsbeamten, da sie das System nun nach Fingerabdrücken durchsuchen können, um die Identität von Personen festzustellen, die in den Schengenraum einreisen oder sich darin bewegen. Dies stellt einen wichtigen Meilenstein für die Sicherheit im Schengenraum dar, da Straftäter, die mehrere oder falsche Identitäten verwenden, einfacher identifiziert werden können. Seit dem 5. März 2018 werden alle neu erfassten Fingerabdrücke mit den bestehenden SIS-Datensätzen abgeglichen, um festzustellen, ob eine Person mehrere Identitäten verwendet. Darüber hinaus führen die elf Schengen-Staaten, die an der ersten Phase dieses Projekts<sup>24</sup> teilnehmen, nun Suchen mit Fingerabdrücken durch. Der von der Kommission vorgeschlagene neue SIS-Rechtsrahmen baut auf der AFIS-Funktion auf und sieht obligatorische Fingerabdruck-Prüfungen vor, wenn die Identität einer Person nicht anderweitig festgestellt werden kann. Die Kommission fordert alle übrigen Mitgliedstaaten auf, die erforderlichen Schritte zu unternehmen, um die neue Funktion für Primärkontrollen an Grenzübergängen sowie für Polizeikontrollen innerhalb des Gebiets zu nutzen. Als weiteren Schritt zur Stärkung des Schengener Informationssystems verabschiedete die Kommission infolge der Schengen-Evaluierungen aus den Jahren 2016 und 2017 zusammen mit diesem Fortschrittsbericht eine neue Version des bestehenden Katalogs von Empfehlungen und bewährten Praktiken.

Auch über die Vorschläge zur Erleichterung des Austauschs von Strafregistereinträgen von Drittstaatsangehörigen in der EU über das **Europäische Strafregisterinformationssystem** und zur Stärkung der Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Recht (**eu-LISA**) werden die Trilogie zwischen den gesetzgebenden Organen fortgeführt.

Im Rahmen der Arbeit zur Verbesserung bestehender Informationssysteme und ihrer Interoperabilität wird die Kommission später im Frühjahr 2018 auf der Grundlage von technischen Studien und einer Folgenabschätzung einen Vorschlag für die Überarbeitung des **Visa-Informationssystems** (VIS) zur Verbesserung der Sicherheit an den Außengrenzen und innerhalb des Schengenraums vorlegen. Diese Überarbeitung des VIS-Rechtsrahmens wird spezifische Maßnahmen zur Interoperabilität umfassen, um die Effizienz der Visa-

---

<sup>24</sup> Österreich, Deutschland, Lettland, Liechtenstein, Luxemburg, Malta, die Niederlande, Polen, Portugal, Slowenien, die Schweiz.

Bearbeitung zu steigern; sie wird außerdem andere in der 2016 durchgeführten Bewertung des VIS festgestellte Probleme angehen.<sup>25</sup>

Die vollständige Umsetzung der Richtlinie über **Fluggastdatensätze** (PNR)<sup>26</sup> stellt in Anbetracht der Schlüsselrolle des Instruments bei der gemeinsamen Reaktion der EU auf die Bedrohung durch Terrorismus und schwerer grenzüberschreitende Kriminalität einen wesentlichen Teil der Bemühungen zur vollständigen Nutzung bestehender Informationssysteme dar. Die Richtlinie muss bis zum 25. Mai 2018 von allen Mitgliedstaaten vollständig umgesetzt werden, damit sie auf Ebene der EU auch effektiv wirken kann. Auf der Tagung des Rates (Justiz und Inneres) am 8. März 2018 betonten die Mitgliedstaaten, die diese Richtlinie bislang noch nicht umgesetzt haben, dass sie alles tun werden, um die festgesetzte Frist einzuhalten. Am 17. April 2018 befanden sich fünf Mitgliedstaaten<sup>27</sup> in einer noch relativ frühen Phase des Umsetzungsprozesses. Die Kommission fordert diese Mitgliedstaaten noch einmal nachdrücklich auf, die Umsetzung rasch voranzutreiben und alle möglichen Schritte zu unternehmen, um sicherzustellen, dass ihre PNR-Zentralstelle und ihre technische PNR-Lösung innerhalb der verbleibenden fünf Wochen bis zum Ende der Frist am 25. Mai 2018 funktionieren.

Die Kommission ermutigt und unterstützt auch weiterhin alle Mitgliedstaaten in ihren Bemühungen, die Richtlinie umzusetzen, auch mit speziellen Kontakten auf politischer und technischer Ebene mit diesen fünf Mitgliedstaaten. Die achte Sitzung zur Umsetzung der PNR-Richtlinie fand am 12. April 2018 statt und bot den Mitgliedstaaten und der Kommission erneut eine Möglichkeit, verbleibende Probleme bei der Umsetzung anzugehen, sowie Angelegenheiten in Bezug auf die Anwendung der PNR-Richtlinie zu untersuchen.

### *3. Schutz gegen chemische, biologische, radiologische und nukleare Bedrohungen und Schutz des öffentlichen Raums*

Der chemische Anschlag in Salisbury hat auf schockierende Art daran erinnert, wie **chemische, biologische, radiologische und nukleare (CBRN) Stoffe** die Sicherheit bedrohen können. Wie bei der Tagung des Europäischen Rats vom 22. und 23. März 2018 gefordert, muss die EU im Einklang mit dem im Oktober 2017 vorgelegten Aktionsplan ihre Widerstandsfähigkeit gegen CBRN-Bedrohungen verstärken.<sup>28</sup> In dem Aktionsplan werden eine Reihe von Maßnahmen festgelegt, um den Zugang zu CBRN-Stoffen einzuschränken, Lücken bei der Erkennung solcher Stoffe zu schließen und die Abwehrbereitschaft gegen sowie die Reaktion auf CBRN-Vorfälle zu verstärken. Die Maßnahmen zielen außerdem darauf ab, die Zusammenarbeit zur Bekämpfung dieser Bedrohungen innerhalb der EU und mit wichtigen internationalen Partnern, einschließlich der NATO, zu fördern. Hierzu gehören der Informationsaustausch, ein gemeinsamer Kapazitätsaufbau, Schulungen und Übungen, auch durch die Zusammenarbeit mit dem von der NATO anerkannten CBRN-Exzellenzzentrum in der Tschechischen Republik. Ein EU-weites CBRN-Sicherheitsnetzwerk wird eingerichtet, um einen Pool aller CBRN-Akteure sowohl auf strategischer als auch auf operativer Ebene zu schaffen. Hier werden die Mitgliedstaaten, die EU-Institutionen, relevante Agenturen und gegebenenfalls wichtige internationale Partner und der private Sektor zusammengebracht. Fünf Mitgliedstaaten müssen noch ihre nationalen CBRN-Sicherheitskoordinatoren benennen und sollten dies unverzüglich tun. Wie vom Europäischen

<sup>25</sup> Mitteilung der Kommission an das Europäische Parlament und den Rat: Anpassung der gemeinsamen Visumpolitik an neue Herausforderungen (COM(2018) 251 final vom 14.3.2018).

<sup>26</sup> Richtlinie (EU) 2016/681 vom 27. April 2016.

<sup>27</sup> Kroatien, Zypern, die Tschechische Republik, Griechenland und Italien.

<sup>28</sup> COM(2017) 610 final vom 18.10.2017.

Rat gefordert, werden die Kommission und die Hohe Vertreterin hinsichtlich der Junitagung des Europäischen Rats im Jahr 2018 über den Fortschritt bei der Umsetzung des CBRN-Aktionsplans und der Stärkung der Kapazitäten zur Bekämpfung von hybriden Bedrohungen berichten.

Im Rahmen der Umsetzung des Aktionsplans zur Förderung des **Schutzes des öffentlichen Raums**<sup>29</sup> insbesondere gegen Terroranschläge organisierten die Kommission und der Ausschuss der Regionen am 8. März 2018 gemeinsam die EU-Bürgermeisterkonferenz über „Städtische Abwehrmaßnahmen gegen den Terrorismus: Lehren aus den jüngsten Anschlägen“, an der fast 200 Personen teilnahmen, auch aus Städten, in denen kürzlich Terroranschläge verübt wurden. Die Teilnehmer der Konferenz konzentrierten sich darauf, welche Lehren aus den jüngsten Terroranschlägen gezogen werden können, und tauschten Erfahrungen und bewährte Praktiken aus. Es konnten Lösungen zur Verbesserung des physischen Schutzes des öffentlichen Raums festgestellt werden, bei denen gleichzeitig die Offenheit und Attraktivität der Städte und des öffentlichen Raums gewahrt bleiben, einschließlich der Umsetzung von Konzepten der „eingebauten Sicherheit“ (Security by Design). Über den Fonds für die innere Sicherheit stehen EU-Mittel für die Umsetzung dieser Lösungen zur Verfügung. Die Kommission prüft derzeit 35 Projektvorschläge, die im Rahmen eines entsprechenden Aufrufs eingegangen sind. Später im Jahr 2018 wird ein Aufruf im Rahmen der Initiative Innovative Maßnahmen für eine nachhaltige Stadtentwicklung mit einem Gesamtbudget von 100 Mio. EUR aus dem Europäischen Fonds für regionale Entwicklung ebenfalls das Thema Sicherheit als Priorität haben. Die Forschung im Bereich Sicherheit trägt ebenfalls zu den Bemühungen zur Verstärkung des Schutzes des öffentlichen Raums bei. 2019 wird ein spezielles Forschungsthema über die „Sicherheit für intelligente und sichere Städte, einschließlich des öffentlichen Raums“ mit einem Budget von 16 Mio. EUR eingeleitet.

#### 4. Cybersicherheit

Die Bekämpfung der Cyberkriminalität und die Verbesserung der Cybersicherheit bleiben auch weiterhin eine Priorität bei EU-Maßnahmen. Um Synergien zu schaffen, vorhandene Kompetenzen und Forschungen zu erweitern und vermarktbarere Lösungen vorzubringen, die die Cybersicherheit des digitalen Binnenmarktes verbessern können, hat die Kommission am 1. Februar 2018 eine Aufforderung zur Einreichung von Vorschlägen für ein mit 50 Mio. EUR ausgestattetes **Pilotprojekt** gestartet, **um den Aufbau eines Netzes von Kompetenzzentren für Cybersicherheit in der EU zu fördern**. Das Netz soll Forschungskompetenzen im Bereich Cybersicherheit aus der gesamten Europäischen Union zusammenbringen (z. B. Universitätslabore, staatliche oder private gemeinnützige Forschungszentren). Das Pilotprojekt wurde in der Gemeinsamen Mitteilung über Cybersicherheit<sup>30</sup> angekündigt, die im September 2017 verabschiedet wurde; die Mittel stammen aus dem Rahmenprogramm Horizont 2020 im Rahmen des geänderten Arbeitsprogramms 2018-2020. Die Frist für die Aufforderung zur Einreichung von Vorschlägen endet am 29. Mai 2018.<sup>31</sup>

Der jüngst festgestellte Einsatz von Cyber-Mitteln zur Manipulation von Verhalten, Vertiefung der gesellschaftlichen Kluft und Untergrabung demokratischer Systeme und

<sup>29</sup> Aktionsplan für einen besseren Schutz des öffentlichen Raums (COM(2017) 612 final vom 18.10.2017).

<sup>30</sup> JOIN(2017) 450 final vom 13.9.2017.

<sup>31</sup> Nähere Informationen zu dieser Aufforderung sind verfügbar unter:  
<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ict-03-2018.html>.

Institutionen unterstreicht die Notwendigkeit, Instrumente beizubehalten, die die Online-Verantwortlichkeit sicherstellen. Dies war ein weiterer Aspekt, der in der Gemeinsamen Mitteilung von 2017 betont wurde, insbesondere durch die Verbesserung der **Verfügbarkeit und Genauigkeit von Daten in der Datenbank „WHOIS“, in der Domainnamen registriert sind**, einer wichtigen Quelle für Ermittlungen im Bereich Cyberkriminalität und Cybersicherheit. Da mit ICANN weiter daran gearbeitet wird, diese Datenbank mit den Datenschutzrichtlinien, insbesondere mit der Datenschutz-Grundverordnung, in Einklang zu bringen, schickte die Kommission ICANN ein Schreiben<sup>32</sup> zu den beiden Zielen, nämlich der Sicherstellung eines schnellen Zugangs zu den Verzeichnissen für die Zwecke des öffentlichen Interesses und die vollständige Einhaltung der EU-Datenschutzrichtlinien. Der ICANN-Beratungsausschuss der Regierungen, in dem nationale Regierungen und die Kommission vertreten sind, verlied seinen Bedenken Ausdruck und forderte ICANN auf, einen kontinuierlichen Zugang zu WHOIS, einschließlich nicht öffentlicher Daten, für Nutzer mit legitimen Zwecken sicherzustellen.

Im Januar 2018 setzte die Kommission eine unabhängige hochrangige Expertengruppe ein, die über politische Optionen zur Bekämpfung von **Fake-News und Desinformationen**, die Online verbreitet werden, beraten und dabei helfen soll, in dieser Hinsicht eine umfassende EU-Strategie zu entwickeln. Am 12. März 2018 gab die Expertengruppe ihren Bericht über einen „multidimensionalen Ansatz für Desinformationen“ heraus, der zur Mitteilung der Kommission zu diesem Thema beiträgt, die in diesem Frühjahr angenommen werden soll.

Am 16. April 2018 **nahm der Rat (Auswärtige Angelegenheiten) die Schlussfolgerungen des Rates über böswillige Cyberangriffe an**. Diese Schlussfolgerungen sind eine praktische Umsetzung der gemeinsamen diplomatischen Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“)<sup>33</sup>, wie die Cyberangriffe *Wannacry* und *NotPetya*. Die Schlussfolgerungen des Rates (Auswärtige Angelegenheiten) unterstreichen die Bedeutung eines offenen, freien, friedlichen und sicheren Cyberspace und betonen, dass die Anwendung des bestehenden internationalen Rechts und die Einhaltung freiwilliger nicht verbindlicher Normen verantwortlichen Verhaltens eines Staates zur Wahrung des Friedens und der Stabilität äußerst wichtig sind.

## 5. Externe Dimension

Um die Sammlung und den Austausch von Informationen zur Bekämpfung von Migrantenschleusung, Menschenhandel, illegalem Waffenhandel und illegalem Handel mit Ölausfuhren aus Libyen zu verbessern, hat der **Rat (Justiz und Inneres)** am 8. und 9. März 2018 den allgemeinen Grundsatz der Beteiligung von Europol und der Europäischen Agentur für die Grenz- und Küstenwache an einem Pilotprojekt für eine „**Kriminalitätsinformationszelle**“, eingebettet in die EU-Marineoperation der Gemeinsamen Sicherheits- und Verteidigungspolitik Sophia (EUNAVFOR MED), gebilligt. Die Kriminalitätsinformationszelle wird einen zeitnahen und zweiseitigen Austausch von Informationen für eine analytische und operative Nutzung zwischen der Operation Sophia und den entsprechenden Agenturen in den Bereichen Justiz und Inneres vereinfachen. Es ist die erste Initiative dieser Art zwischen den Agenturen in den Bereichen Justiz und Inneres und den Missionen oder Operationen der Gemeinsamen Sicherheits- und Verteidigungspolitik. Die praktischen Modalitäten werden derzeit im Rat besprochen, um das Pilotprojekt so

<sup>32</sup> <https://www.icann.org/resources/correspondence/1212685-2018-01-29-en>

<sup>33</sup> Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“) vom 19. Juni 2017.

schnell wie möglich zu starten. Sobald es auf den Weg gebracht wurde, wird das Projekt mittels eines vollständigen Berichts an die Mitgliedstaaten nach sechs Monaten laufend ausgewertet, um den Mehrwert und die Leistung der Kriminalitätsinformationszelle sowie rechtliche und operative Aspekte zu evaluieren, bevor Entscheidungen bezüglich der Fortführung oder Reproduktion in anderen Missionen oder Operationen der Gemeinsamen Sicherheits- und Verteidigungspolitik getroffen werden.

Die Sicherheit im **westlichen Balkan** hat unmittelbaren Einfluss auf die Sicherheit in der EU und ihren Mitgliedstaaten. Die Kommission verabschiedete am 6. Februar 2018 die Mitteilung „Eine glaubwürdige Erweiterungsperspektive für und ein verstärktes Engagement der EU gegenüber dem westlichen Balkan“.<sup>34</sup> Der angehängte Aktionsplan zur Unterstützung des Transformationsprozesses im westlichen Balkan legt sechs thematische Leitinitiativen fest, einschließlich zur Sicherheit und Migration, die bis 2020 abzuschließen sind. Die Arbeiten zur Umsetzung einer Reihe von Maßnahmen zur Verbesserung der Zusammenarbeit mit dem westlichen Balkan zur Bekämpfung des Terrorismus, der Verhütung von gewaltbereitem Extremismus und der Bekämpfung der organisierten Kriminalität, vor allem durch die Entsendung von Europol-Verbindungsbeamten in die gesamte Region<sup>35</sup> und spezielle Expertensitzungen unter Beteiligung der westlichen Balkanstaaten, wie die Sitzung der europäischen Waffenexperten, die am 12. und 13. April 2018 in Sofia stattfand, und dem EU-Dialog zu Drogen („EU Dialogue on Drugs“) am 18. April 2018 in Brüssel, haben begonnen. Der kommende Gipfel in Sofia am 17. Mai 2018 wird auch Gelegenheit bieten, den Fortschritt in dieser Hinsicht zu bewerten.

#### IV. FAZIT

Sechs Monate nach der Annahme einer Reihe praktischer Maßnahmen zur besseren Verteidigung der Bürgerinnen und Bürger der EU gegen terroristische Bedrohungen im Oktober 2017, legt die Kommission zusammen mit dem vorliegenden Fortschrittsbericht eine Reihe weiterer Maßnahmen vor, um den Raum, in dem Terroristen und Straftäter agieren, einzuschränken und die Ermittlungen und Verfolgung von Straftaten und Terroranschlägen zu erleichtern. Die Kommission fordert das Europäische Parlament und den Rat auf, diese Legislativmaßnahmen dringend zu bearbeiten, um die Sicherheit der Bürgerinnen und Bürger zu verbessern.

Die Schaffung eines schützenden Europas bleibt eines der politischen Hauptziele der Union und die Kommission wird weiterhin an einer wirksamen und echten Sicherheitsunion arbeiten, auch im Hinblick auf das informelle Treffen der Staats- und Regierungschefs zur inneren Sicherheit, das laut der Agenda der Führungsspitzen für September 2018 in Wien geplant ist. Die Kommission wird den nächsten Fortschrittsbericht zur Sicherheitsunion im Juni 2018 vorlegen.

---

<sup>34</sup> Mitteilung der Kommission: Eine glaubwürdige Erweiterungsperspektive für und ein verstärktes Engagement der EU gegenüber dem westlichen Balkan, (COM(2018) 65 final).

<sup>35</sup> Bis Sommer 2018 werden drei Europol-Verbindungsbeamte nach Albanien, Bosnien-Herzegowina und Serbien entsandt.