



Straßburg, den 12.12.2017
COM(2017) 779 final

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

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

I. EINFÜHRUNG

Dies ist der zwölfte 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“.

Fast ein Jahr ist seit dem Attentat auf den Berliner Weihnachtsmarkt am 19. Dezember 2016 vergangen, bei dem 12 Menschen ums Leben kamen und 56 Verletzungen davontrugen und das von einer Person begangen wurde, die sich den Grenzschutz- und Strafverfolgungsbehörden entzog, indem sie sich mehrerer Identitäten bediente. Dieser Vorfall und weitere Terroranschläge, die wie die Messerattacke in Marseille im Oktober 2017 unter Nutzung von Mehrfachidentitäten begangen wurden, werfen nicht nur ein Schlaglicht auf die Wichtigkeit eines wirksamen Informationsaustauschs zwischen den Behörden der Mitgliedstaaten, sondern auch auf die maßgebliche Bedeutung der von der Kommission im Frühjahr 2016 in Angriff genommenen Bemühungen¹ um eine Beseitigung der bestehenden Defizite im EU-Informationsmanagement, aufgrund deren es gegenwärtig noch möglich ist, dass Personen in verschiedenen EU-Datenbanken mit unterschiedlichen Identitäten erfasst sind. Die Legislativvorschläge für Verordnungen² über die Interoperabilität von Informationssystemen, die im Rahmen eines Pakets zusammen mit dem vorliegenden Bericht vorgelegt worden sind, sollen Terroristen und Straftätern den Spielraum zur Nutzung der derzeit bestehenden Lücken für Identitätsdiebstahl nehmen, um auf diese Weise zu einem verbesserten Schutz der EU-Außengrenzen, einer Stärkung der inneren Sicherheit und zu einer besseren Steuerung der Migration beizutragen.³ Die Vorschläge bedeuten einen grundlegenden Wandel nicht nur für die Art und Weise, in der Informationen in den Bereichen Sicherheits- und Grenzmanagement sowie Migrationssteuerung gehandhabt werden, sondern auch für deren Bereitstellung gegenüber den einzelstaatlichen Behörden, damit diesen die Informationen zur Verfügung stehen, wann und wo sie diese benötigen. Angesichts der zentralen Bedeutung, die diesen Vorschlägen für einen wirksameren Grenzschutz und eine effektivere Strafverfolgung zukommt, appelliert die Kommission nunmehr an die Legislativorgane, die Gesetzgebungsvorschläge zur Interoperabilität mit oberster Priorität zu behandeln und außerdem rasch Einigung über die übrigen vorgelegten Legislativvorschläge zu erzielen, die sich auf einzelne Informationssysteme beziehen, um diejenigen mit den nötigen Informationen auszustatten, die sich an vorderster Front um einen wirksamen Schutz unserer Bürger bemühen.

Im Mittelpunkt dieses Berichts stehen daher die nächsten auf solidere und intelligenter Informationssysteme für das Sicherheits- und das Grenzmanagement und die Migrationssteuerung zielenden Schritte, die es zu ergreifen gilt, um die Datenarchitektur der EU-Informationssysteme wirksamer und effizienter zu gestalten und dabei allen datenschutzrechtlichen Erfordernissen Rechnung zu tragen.

In diesem Bericht wird daneben eine Bilanz einer Reihe von Maßnahmen zur Maximierung des Nutzens bestehender Informationssysteme gezogen, die gesetzgeberische Tätigkeiten ebenso erfasst wie die laufenden Bemühungen um deren vollumfängliche Umsetzung und die

¹ COM(2016) 205 final vom 6.4.2016.

² COM(2017) 793 final und COM(2017) 794 final vom 12.12.2017.

³ COM(2017) 261 final vom 16.5.2017.

bessere Nutzung von EU-weiten Informationssystemen. Bei seiner im Oktober 2017 gezogenen Bilanz hinsichtlich der Umsetzung des Bratislava-Fahrplans⁴ nahm der Europäische Rat die erheblichen Fortschritte zur Kenntnis, die sich innerhalb der EU insbesondere auf dem Gebiet der inneren Sicherheit auf vier Feldern verzeichnen ließen: verstärkte Zusammenarbeit und gesteigerter Informationsaustausch, vermehrter Abgleich und stärkere Vernetzung von Datenbanken, Entwicklung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und systematische Bemühungen, Radikalisierung entgegenzuwirken. In diesem Bericht wird dargelegt, dass in all diesen Bereichen in den zurückliegenden beiden Monaten weitere Fortschritte erzielt worden sind.

II. SOLIDERE UND INTELLIGENTERE INFORMATIONSSYSTEME FÜR DAS SICHERHEITS- UND DAS GRENZMANAGEMENT SOWIE FÜR DIE MIGRATIONSSTEUERUNG

Jüngsten Umfragen zufolge stößt ein vermehrter EU-weiter Austausch von Informationen zur Bekämpfung von Terrorismus und organisiertem Verbrechen bei den EU-Bürgern auf große Zustimmung.⁵ Die von der EU bereitgestellten Informationen spielen eine entscheidende Rolle bei der Unterstützung einzelstaatlicher Behörden beim Management der Außengrenze, bei der Kriminalitäts- und Terrorismusbekämpfung und der Eindämmung der irregulären Migration. Zur Maximierung dieses Zusatznutzens für die EU müssen die von den EU-Systemen bereitgestellten Angaben lückenlos, genau und zuverlässig sein. Gegenwärtig bieten sich diese Informationen fragmentiert und komplex dar, und ihre Handhabung bereitet Probleme.

Zur Beseitigung dieser Mängel⁶ haben sich – darin der Mitteilung der Kommission vom April 2016 folgend – die Arbeiten auf drei Bereiche konzentriert: Maximierung des Nutzens, der sich aus den bestehenden Informationssystemen ziehen lässt; Entwicklung neuer und ergänzender Systeme zum Schließen vorhandener Lücken; und Verbesserung der Interoperabilität der Informationssysteme.

1. Auf dem Weg zur Interoperabilität von Informationssystemen

Zunächst werden die vorgeschlagenen Maßnahmen die Beamten vor Ort dabei unterstützen, **aus den vorhandenen Daten größtmöglichen Nutzen zu ziehen**. Ein *EU-weites Suchportal* wird eine zentrale Anlaufstelle bereitstellen, über die sich mehrere EU-Informationssysteme⁷ sowie die maßgeblichen Europol-Daten und die Interpol-Systeme – im Umfang der Zugriffsberechtigungen des Nutzers – gleichzeitig durchsuchen lassen. Die Beamten vor Ort erhalten so einen effizienten, raschen und nahtlosen Zugang zu den Daten, die sie zur Wahrnehmung ihrer Aufgabe benötigen; zugleich entfällt die bisherige, komplizierte Notwendigkeit, sich zu entscheiden, welche Datenbank im konkret vorliegenden Fall abgefragt werden soll.

⁴ <http://www.consilium.europa.eu/media/21597/bratislava-implementation-report.pdf> (in englischer Sprache)

⁵ Vgl. hierzu die Sonderausgabe 464b des Eurobarometer vom 12. Dezember 2017 zur Einstellung der EU-Bürgerinnen und -Bürger zu Fragen der Sicherheit: <http://ec.europa.eu/comfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/1569> (in englischer Sprache).

⁶ COM(2016) 205 final vom 6.4.2016.

⁷ Das Schengener Informationssystem, das Eurodac-System, das Visa-Informationssystem (VIS), das künftige Einreise-/Ausreiseregister (EES), das vorgeschlagene Europäische Reiseinformations- und -genehmigungssystem (ETIAS) und das vorgeschlagene Europäische Strafregisterinformationssystem (ECRIS) für Drittstaatsangehörige.

Zum Zweiten werden die vorgeschlagenen Maßnahmen durch die Verwendung biometrischer Daten die einzelstaatlichen Behörden in die Lage versetzen, **die Nutzung von Mehrfachidentitäten aufzudecken sowie Identitätsbetrug zu begegnen**. Ein *gemeinsamer Dienst für den Abgleich biometrischer Daten* wird die Suche nach und den Vergleich von biometrischen Daten aus mehreren Zentralsystemen ermöglichen⁸, während ein *gemeinsamer Speicher für Identitätsdaten* den Verbund aus biografischen und biometrischen Identitätsdaten von Drittstaatsangehörigen enthalten wird, die in den EU-Informationssystemen gespeichert sind⁹. Aufbauend auf diesen beiden Interoperabilitätskomponenten wird ein *Mehrfachidentitätsdetektor* prüfen, welche Daten zu einer abgefragten Identität in mehr als einem der angeschlossenen Systeme vorhanden sind.¹⁰ Jedes Mal, wenn Einwanderungs- und Ausländerbehörden eine Person in EU-Informationssystemen erfassen oder Polizei- und Grenzschutzbeamte die Daten zu einer Person mit den Einträgen in diesen Systemen abgleichen, wird ihnen mitgeteilt, ob diese bereits unter einer anderen Identität bekannt ist oder sich mehrerer Identitäten bedient. Dies wird dazu beitragen, die gegenwärtigen Lücken und Schwachpunkte zu beseitigen, die Terroristen wie auch sonstige Straftäter auszunutzen trachten, indem sie sich hinter einer falschen Identität oder mehreren Identitäten verbergen.

Drittens werden die vorgeschlagenen Maßnahmen Polizeibeamte in die Lage versetzen, **innerhalb ihres Hoheitsgebiets rasche und wirksame Identitätskontrollen** durchzuführen. Bei solchen Kontrollen werden Polizeibeamte Zugang zu den Identitätsdaten von Drittstaatsangehörigen, deren Daten in EU-Informationssystemen verzeichnet sind, und damit auch die Möglichkeit zur eindeutigen Identifizierung und zur Erkennung von Mehrfachidentitäten erhalten. Dies wird die Wirksamkeit von Kontrollen innerhalb des Hoheitsgebiets der Mitgliedstaaten erheblich steigern, wie dies auch die Empfehlung der Kommission zu verhältnismäßigen Polizeikontrollen und zur polizeilichen Zusammenarbeit im Schengen-Raum¹¹ vorsieht.

Zur Ergänzung dieser Interoperabilitätskomponenten schlägt die Kommission darüber hinaus vor, den **Zugang von Strafverfolgungsbehörden zu Systemen** außerhalb des Bereichs Strafverfolgung durch die Einführung eines neuen zweistufigen Datenabfrageverfahrens **zu erleichtern und zu straffen**. Bereits nach den derzeitigen Bestimmungen verfügen Strafverfolgungsbehörden über die Möglichkeit, Informationssysteme außerhalb des Bereichs der Strafverfolgung zum Zwecke der Prävention, Ermittlung, Erkennung oder auch Verfolgung terroristischer oder anderweitiger schwerwiegender Straftaten abzufragen. Allerdings gelten für die jeweiligen Systeme unterschiedliche Zugangsvoraussetzungen und Sicherheitsvorkehrungen, und manche der bestehenden Regelungen erschweren die rechtmäßige Nutzung der betreffenden Systeme durch diese Behörden. Nach dem neuen zweistufigen Datenabfrageverfahren würde ein Vollstreckungsbeamter zunächst sämtliche Systeme prüfen, die ihre Daten im *gemeinsamen Speicher für Identitätsdaten* hinterlegen, um

⁸ Das Schengener Informationssystem, das Eurodac-System, das Visa-Informationssystem (VIS), das künftige Einreise-/Ausreisensystem (EES) und das vorgeschlagene Europäische Strafregisterinformationssystem (ECRIS) für Drittstaatsangehörige.

⁹ Das Eurodac-System, das Visa-Informationssystem (VIS), das künftige Einreise-/Ausreisensystem (EES), das vorgeschlagene Europäische Reiseinformations- und -genehmigungssystem (ETIAS) und das vorgeschlagene Europäische Strafregisterinformationssystem (ECRIS) für Drittstaatsangehörige.

¹⁰ Das Schengener Informationssystem, das Eurodac-System, das Visa-Informationssystem (VIS), das künftige Einreise-/Ausreisensystem (EES), das vorgeschlagene Europäische Reiseinformations- und -genehmigungssystem (ETIAS) und das vorgeschlagene Europäische Strafregisterinformationssystem (ECRIS) für Drittstaatsangehörige.

¹¹ C(2017) 3349 final vom 12.5.2017.

in Erfahrung zu bringen, ob in irgendeinem der angeschlossenen Systeme Informationen zur betreffenden Person gespeichert sind. Aus Datenschutzgründen würde die Antwort lediglich „Treffer“ oder „Kein Treffer“ lauten. Der Beamte erhielte dabei keinen Zugang zu irgendwelchen in einem der Systeme vorhandenen Daten, erlangte jedoch die entscheidende Kenntnis davon, ob und ggf. an welchem Ort solche Daten existieren. In einem zweiten Schritt wäre der Beamte sodann in der Lage, einen vollständigen Zugriff auf das Informationssystem bzw. die Informationssysteme zu beantragen, die Treffer generierten, wobei er für jedes dieser Systeme im Einklang mit den jeweils geltenden Bestimmungen einen gesonderten Zugangsantrag zu stellen hätte. Wie bereits heute müsste der Beamte sein Interesse an einem Zugang zum System im Einklang mit den für das jeweilige Informationssystem geltenden Zugriffsrechten und den Grundsätzen der Zweckbindung begründen, wobei ein anschließender Vollzugriff an die vorherige Genehmigung durch eine entscheidungsbefugte Stelle geknüpft wäre und weiterhin eine spezifische Nutzerkennung und Anmeldedaten erforderte. Sobald ein solches zweistufiges Datenabfrageverfahren zur Anwendung gelangt, wird sich eine vorangehende Suche in einzelstaatlichen Datenbanken und in automatisierten Fingerabdruck-Identifizierungssystemen anderer Mitgliedstaaten gemäß Beschluss 2008/615/JI („Überprüfung nach den Prüm-Kriterien“) erübrigen.

Mit den Vorschlägen zur Interoperabilität **werden Grundrechte wie insbesondere das Recht auf Schutz personenbezogener Daten gewahrt und propagiert**. Durch die Schaffung umfassender Rahmenbedingungen für den Schutz personenbezogener Daten in der EU und bedeutende Entwicklungen auf dem Gebiet der Technologie und der IT-Sicherheit lässt sich der Grundsatz der Zweckbindung beim Zugriff auf Daten und bei deren Verwendung im vollen Einklang mit der Grundrechtecharta und der jüngsten Rechtsprechung des Europäischen Gerichtshofs leichter umsetzen. Die vorgeschlagenen Maßnahmen werden keine Vernetzung der einzelnen Systeme zur Folge haben. Vielmehr wird jedes System seine spezifische Zweckbindung sowie seine Zugangsbestimmungen und Vorschriften zur Datenvorhaltung bewahren. Die vorgeschlagenen Maßnahmen werden auch zu keiner vermehrten Erfassung neuer Daten führen. Sie bieten eine zielgerichtete und durchdachte Möglichkeit zur Verwendung von in den Systemen der EU bereits gespeicherten Informationen zum größtmöglichen Nutzen.

Die Legislativvorschläge sind das Ergebnis eines **inkluisiven und transparenten Prozesses**, der mit der Mitteilung der Kommission über solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit vom April 2016 angestoßen und von einer hochrangigen Sachverständigengruppe¹² weiterverfolgt wurde, welche sich mit den gesetzlichen, technischen und operativen Herausforderungen befasste, die mit den verschiedenen Optionen zur Erzielung von Interoperabilität verbunden sind.

¹² Die Einrichtung der Sachverständigengruppe erfolgte gemäß dem Kommissionsbeschluss 2016/C 257/03 vom 17.6.2016. Die Gruppe vereinte Experten aus Mitgliedstaaten und assoziierten Schengen-Staaten sowie aus der EU-Agentur eu-LISA, Europol, dem Europäischen Unterstützungsbüro für Asylfragen (EASO), der Europäischen Agentur für die Grenz- und Küstenwache (Frontex) und der Agentur der Europäischen Union für Grundrechte (FRA). Der EU-Koordinator für die Terrorismusbekämpfung und der Europäische Datenschutzbeauftragte wirkten darin als Vollmitglieder mit. Vertreter des Sekretariats des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments und des Generalsekretariats des Rates nahmen daran als Beobachter teil. Der Abschlussbericht der Sachverständigengruppe ist nachzulesen unter: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1> (in englischer Sprache). In den zugehörigen Anhängen findet sich eine Zusammenfassung eines Berichts der FRA sowie Erklärungen des Europäischen Datenschutzbeauftragten und des EU-Koordinators für die Terrorismusbekämpfung.

Die Legislativvorschläge enthalten ausführliche Bestimmungen hinsichtlich der **an den Rechtsinstrumenten vorzunehmenden Änderungen**; hierbei handelt es sich um derzeit nicht weiter überarbeitete, von den Legislativorganen verabschiedete Texte wie insbesondere den Schengener Grenzkodex, die Verordnung in Bezug auf die Nutzung des Einreise-/Ausreisensystems und die Rechtsakte, denen das Visa-Informationssystem unterliegt. Die sonstigen hiervon erfassten Instrumente¹³ sind Gegenstand von im Europäischen Parlament und im Rat derzeit geführten Verhandlungen. In Bezug auf diese Instrumente lassen sich die erforderlichen Änderungen daher zum gegenwärtigen Zeitpunkt noch nicht darlegen. Die Kommission wird solche Änderungen zu jedem dieser Instrumente innerhalb von zwei Wochen nach Erzielung einer politischen Übereinkunft über den betreffenden Verordnungsentwurf vorlegen. Sie appelliert an die Legislativorgane, bei den laufenden Verhandlungen über diese Instrumente rasch zu einer Übereinkunft zu gelangen.

2. Entwicklung neuer und ergänzender Maßnahmen zur Schließung vorhandener Lücken

Zusätzlich zu den vorstehend dargelegten neuen Maßnahmen zur Interoperabilität bedarf es zwingend weiterer Fortschritte beim Schließen der aktuellen Informationslücken, welche die Kommission in ihrer Mitteilung von April 2016 in Bezug auf Besucher des Schengen-Raums aufgezeigt hat, die einem Drittstaat angehören. Die abschließenden Formulierungen der Verordnung über das **EU-Einreise-/Ausreisensystem**¹⁴ (EES) und die Verordnung zur Änderung des Schengener Grenzkodex¹⁵ zu dessen Angleichung an das EES¹⁵ wurden von den Legislativorganen Ende November verabschiedet und werden Ende 2017 in Kraft treten. Nach dieser Entwicklung soll das System 2018 seinen Betrieb aufnehmen, um sicherzustellen, dass es bis 2020 seine volle Funktionsfähigkeit erlangt haben wird.

Eine weitere Informationslücke – in Bezug auf Drittstaatsangehörige, die kein Visum benötigen – war Gegenstand des Legislativvorschlags der Kommission von November 2016 zur Schaffung eines neuen IT-Großsystems in Gestalt des **Europäischen Reiseinformations- und -genehmigungssystem (ETIAS)**. Der Rat hat sich im Juni 2017 auf eine allgemeine Ausrichtung verständigt, und das dem Europäischen Parlament erteilte Verhandlungsmandat wurde am 25. Oktober 2017 bestätigt. Am selben Tag wurden im Trilog Verhandlungen aufgenommen, die am 16. November 2017 und am 29. November 2017 fortgeführt wurden. Der nächste politische Trilog ist für den 12. Dezember 2017 geplant. Die Kommission appelliert an beide Legislativorgane, im Einklang mit den Schlussfolgerungen des Europäischen Rates von Dezember 2016 und der Gemeinsamen Erklärung bis Ende 2017 zu einer politischen Einigung über das Dossier zu gelangen.

3. Maximierung des Nutzens bestehender Informationssysteme

(a) Laufende Legislativtätigkeit zur Stärkung bestehender Informationssysteme

Im Rahmen der von der Kommission unternommenen Bemühungen um eine Maximierung des Potenzials der bestehenden EU-Informationssysteme hat die Kommission im Dezember

¹³ Die vorgeschlagenen Verordnungen über das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) und das Europäische Strafregisterinformationssystem für Drittstaatsangehörige, die Verordnungen über Eurodac, das Schengener Informationssystem und eu-LISA sowie die sich daraus ergebenden Änderungen der vorgeschlagenen Verordnung über das ETIAS, die die Verordnung über die Europäische Agentur für die Grenz- und Küstenwache betreffen.

¹⁴ Verordnung (EU) 2017/2226 vom 30.11.2017.

¹⁵ Verordnung (EU) 2017/2225 vom 30.11.2017.

2016 drei Legislativvorschläge zur Stärkung des **Schengener Informationssystems (SIS)**¹⁶ angenommen. Diese sehen wesentliche Maßnahmen zur verstärkten Bekämpfung von Terrorismus vor, beispielsweise durch die Einführung einer Verpflichtung der Mitgliedstaaten zur SIS-Ausschreibung von Personen, nach denen in Zusammenhang mit einer terroristischen Straftat gefahndet wird. Bei den im Europäischen Parlament und im Rat geführten Diskussionen wurde daneben der Bedarf nach Weitergabe von im SIS erfassten Informationen über terroristische Straftaten an Europol angesprochen, wobei Änderungen vorgeschlagen wurden, die es Europol und den Mitgliedstaaten ermöglichen sollen, zusätzliche Informationen über SIS-Treffer mit Terrorismusbezug auszutauschen, und die Europol in die Lage versetzen sollen, Informationen über neu erstellte Ausschreibungen und diesbezügliche Treffer mit Europol's Datenbanken und Arbeitsdateien zu Analysezwecken abzugleichen. Die Verhandlungen zwischen dem Europäischen Parlament und dem Rat über diese Vorschläge wurden am 16. November 2017 aufgenommen. Angesichts der Bedeutung dieser Vorschläge fordert die Kommission die Legislativorgane nachdrücklich dazu auf, bis Anfang 2018 hinsichtlich der Vorschläge zu einer Einigung zu gelangen.

Parallel dazu wurden, wie seit 2016 geplant, die Arbeiten zur Stärkung des SIS durch die Einführung eines **automatisierten Fingerabdruck-Identifizierungssystems (AFIS)** fortgeführt. Endanwender des SIS (wie Polizei- und Grenzschutzbeamte) erhalten damit die Möglichkeit, das SIS anhand von Fingerabdruckdaten abzufragen und so zuverlässige Angaben auch über solche Personen zu erhalten, die unter einer falschen Identität reisen. Neun Mitgliedstaaten haben sich dazu bereit erklärt, an der ersten Phase der Einführung des AFIS teilzunehmen, die im März 2018 beginnen soll. Die flächendeckende Einführung in allen Mitgliedstaaten, die das SIS nutzen, soll im weiteren Verlauf des Jahres abgeschlossen sein.

Über den Legislativvorschlag zur Stärkung des **Eurodac**¹⁷-Systems sind Trilogie im Gange. Eurodac stellt eines der künftig von den Interoperabilitätskomponenten erfassten Informationssysteme dar, weshalb es wichtig ist, dass die Legislativorgane über dieses Dossier rasch Einigkeit erzielen. In der Mitteilung, in der der Beitrag der Kommission zum Treffen der EU-Führungsspitzen über das weitere Vorgehen in Bezug auf die externe und die interne Dimension der Migrationspolitik¹⁸ dargelegt ist, ruft die Kommission dazu auf, den Vorschlag bis März 2018 zu verabschieden.

Um den Spielraum von Terroristen und Straftätern weiter einzuschränken, hat die Kommission am 29. Juni 2017 einen ergänzenden Vorschlag zur Erleichterung des Austauschs von Strafregister-Informationen über Drittstaatsangehörige in der EU über das **Europäische Strafregisterinformationssystem (ECRIS)**¹⁹ vorgelegt. Der Rat (Justiz und Inneres) hat am 8. Dezember 2017 eine allgemeine Ausrichtung sowohl zu der vorgeschlagenen Richtlinie²⁰ als auch zu der geplanten Verordnung angenommen. Die im Trilog geführten Gespräche zwischen den Legislativorganen könnten beginnen, sobald das Europäische Parlament dessen Verhandlungsmandat bezüglich beider ECRIS-Vorschläge genehmigt. Die Kommission appelliert an beide Legislativorgane, zu einer raschen Einigung über die Vorschläge zu gelangen.

¹⁶ COM(2016) 881 final, COM(2016) 882 final und COM(2016) 883 final vom 21.12.2016.

¹⁷ COM(2016) 272 final vom 4.5.2016.

¹⁸ COM(2017) 820 final vom 7.12.2017.

¹⁹ COM(2017) 344 final vom 29.6.2017.

²⁰ COM(2016) 7 final vom 19.1.2016.

Am 29. Juni 2017 hat die Kommission einen Vorschlag zur Änderung des **Mandats der Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts**²¹ angenommen. Die Agentur sollte damit beauftragt werden, zur Entwicklung der Interoperabilität zwischen IT-Großsystemen beizutragen. Vor diesem Hintergrund zielt der Vorschlag darauf, die Verordnung, auf der die Agentur gründet, im Sinne der sich aus der Evaluierung der Agentur ergebenden Empfehlungen zu überarbeiten, die Funktionsweise der Agentur zu verbessern, sie zu stärken und ihr größeres Gewicht zu verleihen, damit sie den heutigen Anforderungen auf EU-Ebene gewachsen ist. Ebenso zielt der Vorschlag darauf, sich aus politischen, rechtlichen oder sachlichen Entwicklungen ergebende Änderungen aufzunehmen und insbesondere widerzuspiegeln, dass die Agentur mit neuen Systemen betraut werden wird. Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments hat sein Verhandlungsmandat am 7. Dezember 2017 angenommen, und der Rat erzielte am selben Tag Einigung über eine allgemeine Ausrichtung.

(b) Gewährleistung der umfassenden Implementierung bestehender Informationssysteme

Ein wichtiges Instrument im Kampf gegen Terrorismus und organisiertes Verbrechen stellt die **Richtlinie über europäische Fluggastdatensätze (PNR)**²² dar. Obwohl in allen Mitgliedstaaten weiterhin Arbeiten zur Gewährleistung der vollumfänglichen Umsetzung der Richtlinie bis zum Stichtag 25. Mai 2018 im Gange sind, bestehen auch ein Jahr, nachdem im November 2016 der Plan zur Umsetzung der PNR²³ beschlossen wurde, zwischen den Mitgliedstaaten erhebliche Diskrepanzen fort, was den Stand der Einrichtung ihrer nationalen PNR-Systeme angeht. Der Stichtag für die Umsetzung naht mit großen Schritten. Diese Anstrengungen sind daher unbedingt zu intensivieren, um bis zum 25. Mai 2018 zu einem erfolgreichen Abschluss zu gelangen. Von besonderer Bedeutung ist dabei die Einrichtung der Verfahren und Kommunikationskanäle, die es den einzelstaatlichen PNR-Zentralstellen ermöglichen, jegliche PNR-Daten von Interesse an die entsprechenden Stellen in anderen Mitgliedstaaten sowie an Europol weiterzugeben. Dieses essenzielle EU-Sicherheitsinstrument wird erst dann sein ganzes Potenzial entfalten können, wenn alle Mitgliedstaaten über funktionierende PNR-Systeme verfügen und in der Lage sind, Daten wirksam sowohl untereinander als auch mit Europol auszutauschen. Zum 15. November 2017 bietet sich diesbezüglich das folgende Bild dar:

- Sieben Mitgliedstaaten verfügen bereits über sowohl die rechtlichen als auch die technischen Voraussetzungen für die Erfassung und Verarbeitung von PNR-Daten. Allerdings bedarf es in der Mehrzahl dieser Mitgliedstaaten noch Anpassungen der Gesetzesgrundlage, um allen in der PNR-Richtlinie gestellten Anforderungen zu entsprechen.
- 13 Mitgliedstaaten befinden sich in einem Zwischenstadium der Umsetzung. Vier darunter verfügen über eingerichtete und ausgestattete PNR-Zentralstellen, nehmen bislang jedoch in Ermangelung einer Gesetzesgrundlage für die Sammlung personenbezogener Daten keine Erfassung und Verarbeitung realer PNR-Daten vor. Die übrigen neun Mitgliedstaaten befinden sich in unterschiedlichen Stadien der Fertigstellung der Entwicklung oder Einrichtung ihrer PNR-Zentralstelle und der technischen Lösung, die zur Verarbeitung von PNR-Daten nach den Anforderungen der PNR-Richtlinie verwendet werden soll, während die Einbindung von Luftfahrtunternehmen noch im Gange ist.

²¹ COM(2017) 352 final vom 29.6.2017.

²² Richtlinie (EU) 2016/681 vom 27.4.2016.

²³ SWD(2016) 426 final vom 28.11.2016.

Allerdings haben einige dieser neun Mitgliedstaaten Gesetze zum Umgang mit PNR bereits verabschiedet.

- Sieben Mitgliedstaaten sind im Umsetzungsprozess noch nicht hinreichend vorangeschritten und müssen erst noch die Verwaltungsarchitektur ihrer PNR-Zentralstellen definieren und/oder die diesbezügliche Gesetzgebung ihren Parlamenten vorlegen und/oder mit der Einrichtung der technischen Lösung beginnen, die von den PNR-Zentralstellen genutzt werden soll, und/oder den Prozess zur Herstellung einer Verbindung mit Luftfahrtunternehmen in Gang setzen.

Die Kommission unterstützt die Mitgliedstaaten auch weiterhin bei deren Bemühungen um eine zeitnahe Umsetzung der Richtlinie. Das sechste Treffen zur Umsetzung der PNR-Richtlinie fand am 3. Oktober 2017 statt und bot den Sachverständigen der Mitgliedstaaten Gelegenheit, einander wie auch die Kommission über deren Fortschritt beim Umsetzungsprozess auf den neuesten Stand zu bringen und gewonnene Erkenntnisse, bewährte Vorgehensweisen und praktische Erfahrungen weiterzugeben.

Finanzielle Unterstützung wurde geleistet über die einzelstaatlichen Programme und EU-Maßnahmen im Rahmen des Fonds für innere Sicherheit – Polizei zur Unterstützung der Einrichtung funktionierender PNR-Zentralstellen auf einzelstaatlicher Ebene und zur Ermöglichung des Austauschs von PNR-Daten untereinander im Einklang mit der PNR-Richtlinie²⁴.

Fortgesetzt werden auch die Arbeiten zur Sicherstellung einer vollständigen Umsetzung der **Beschlüsse zum Prümer Vertrag**²⁵ über den Austausch von Fingerabdrucks-, DNA- und Fahrzeugregisterdaten. Wenn auch in der Mehrzahl der Mitgliedstaaten diesbezüglich Fortschritte erzielt wurden, musste die Kommission von ihren Befugnissen in Sachen Verstoßverfahren Gebrauch machen. Die Kommission sandte mit Gründen versehene Stellungnahmen am 18. Mai 2017 an Kroatien, Irland und Italien und am 5. Oktober 2017 an Griechenland. Parallel dazu leistete die Kommission den Mitgliedstaaten weiterhin Unterstützung durch die Bereitstellung von Mitteln für die Umsetzung innerhalb der nationalen Programme im Rahmen des Fonds für innere Sicherheit – Polizei. Die Kommission hat zusätzliche 22 Mio. EUR für diese nationalen Programme für 2017 bereitgestellt, und diese Mittel können für die Umsetzung des Prümer Vertrags verwendet werden.

(c) Unterstützung für eine bessere Nutzung bestehender Informationssysteme

Zusätzlich zur Stärkung bestehender Systeme und die Gewährleistung ihrer vollumfänglichen Umsetzung bemüht sich die Kommission auch nach Kräften um eine bessere Nutzung

²⁴ Wie in „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Fünfter Fortschrittsbericht“ angekündigt, hat die Haushaltsbehörde den Unionshaushalt für das Jahr 2017 mit zusätzlichen Mitteln in Höhe von 70 Mio. EUR im Rahmen des Fonds für innere Sicherheit – Polizei zur Unterstützung von PNR-bezogenen Maßnahmen im Zeitraum 2017-2020 ausgestattet. Diese zusätzlichen Ressourcen wurden als Zugabe zu den nationalen Programmen der Mitgliedstaaten nach dem Verteilerschlüssel des Fonds’ verteilt. Was die Maßnahmen auf Unionsebene angeht, hat das laufende Projekt „PIU.net“, das aufgrund einer Aufforderung zur Einreichung von Vorschlägen 2016 im Rahmen des Fonds für innere Sicherheit – Polizei ausgewählt wurde (mit einer Zuwendung von maximal 3,78 Mio. EUR) zum Ziel, eine technische Lösung zur Erleichterung des Austauschs von PNR-Daten zwischen PNR-Zentralstellen der Mitgliedstaaten bereitzustellen. Im November 2017 hat die Kommission eine mit Mitteln in Höhe von insgesamt 1,5 Mio. EUR ausgestattete zusätzliche Aufforderung zur Einreichung von Vorschlägen für Schulung, Sensibilisierung und sonstige Maßnahmen zum Aufbau von Kapazitäten zielende Maßnahmen veröffentlicht, die sich an die Mitarbeiter der PNR-Zentralstellen richtet.

²⁵ Beschlüsse 2008/615/JI und 2008/616/JI des Rates vom 23.6.2008.

bestehender Informationssysteme. Im Rahmen des **Schengen-Evaluierungsmechanismus**²⁶ finden in den Mitgliedstaaten alle fünf Jahre Beurteilungen vor Ort der Umsetzung des SIS statt, die von Sachverständigen des jeweiligen Mitgliedstaates oder der Kommission durchgeführt werden. 2017 wurden solche Evaluierungsbesuche in Dänemark, Island, Schweden, Portugal, Spanien, Kroatien, Norwegen und im Vereinigten Königreich durchgeführt. Jegliche bei den Evaluierungen festgestellte Umsetzungsprobleme werden in Form von Empfehlungen des Rates an den betreffenden Mitgliedstaat angegangen. In Bezug auf frühere Empfehlungen verzeichnete Fortschritte sind ebenfalls Teil der von den Evaluierungs-Teams bei ihren Besuchen vor Ort durchgeführten Kontrollen. Die Kommission wird auf Grundlage der Erkenntnisse, die bei den bislang durchgeführten Schengen-Evaluierungen zur Verwendung des Schengen-Informationssystems gewonnen worden sind, eine Reihe von **bewährten Vorgehensweisen und gewonnenen Erkenntnissen**, die allen Mitgliedstaaten bei der Verbesserung der Verwertung bestehender Informationssysteme von zusätzlichem Nutzen sind, für spätere Gespräche mit den Mitgliedstaaten ausarbeiten.

Zur weiteren Verbesserung der Informationsströme sollten die Mitgliedstaaten für einen verbesserten Informationsaustausch mit Europol umfassend von technischen Lösungen Gebrauch machen. Eine Automation des Prozesses des Hochladens von Daten auf das **Europol-Informationssystem** zu Zwecken des Datenabgleichs kann den Austausch von maßgeblichen und aktuellen Informationen mit Europol und weiteren Mitgliedstaaten verbessern. Sogenannte „Data Loaders“ stellen ein technisches Instrument für solch ein automatisiertes Hochladen von Daten bereit. Europol hat solche Data Loaders entwickelt, um den Mitgliedstaaten eine Möglichkeit zu schaffen, ihre Leistung beim Hochladen, Aktualisieren und Löschen von Daten im Europol-Informationssystem zu verbessern. Data Loaders befinden sich in mehreren Mitgliedstaaten bereits im Einsatz.²⁷ Um einer sehr viel größeren Gruppe von Polizeibeamten den Zugang zu Europol-Daten zu eröffnen, richtet sich ein laufendes Pilotprojekt, an dem fünf Mitgliedstaaten (Spanien, Estland, Finnland, Griechenland, Polen) beteiligt sind, auf die Verwendung von **QUEST**, eine Systemschnittstelle, über die sich automatische Abfragen in Europol-Daten aus einzelstaatlichen polizeilichen Informationssystemen integrieren lassen. Die Schnittstelle soll Anfang 2018 nach erfolgter Validierung durch den europäischen Datenschutzdienst und nach Abschluss von operativen Tests durch die Mitgliedstaaten in Betrieb genommen werden.

Die Kommission hat eine Studie zur Untersuchung der Vollständigkeit und Übereinstimmung der Maßnahmen der Mitgliedstaaten zur Umsetzung des **schwedischen Rahmenbeschlusses**²⁸ in Auftrag gegeben, der einen gemeinsamen Rechtsrahmen für den Austausch von Informationen zwischen Strafverfolgungsbehörden der Mitgliedstaaten bereitstellt. Die Ergebnisse werden voraussichtlich im ersten Quartal 2018 vorliegen und werden darauf geprüft werden, ob weitere Maßnahmen erforderlich sind. Am 3. Oktober 2017 hat die Kommission Luxemburg wegen des Versäumnisses der Mitteilung der zur Umsetzung dieses Beschlusses getroffenen einzelstaatlichen Maßnahmen eine mit Gründen versehene Stellungnahme übermittelt.

²⁶ Verordnung (EU) Nr. 1053/2013 des Rates vom 7.10.2013.

²⁷ Beispielsweise: durch Belgien, Finnland, Polen, das Vereinigte Königreich und jüngst auch durch die Tschechische Republik und Kroatien.

²⁸ Rahmenbeschluss des Rates 2006/960 vom 18.12.2006.

III. UMSETZUNG WEITERER PRIORITÄTEN IM BEREICH DER SICHERHEIT

Neben den Bemühungen um die Schließung von Informationslücken und die Stärkung von Informationssystemen wurden auch in einer Reihe weiterer Felder der Sicherheitsunion die Arbeiten fortgeführt.

1. Maßnahmen für einen besseren Schutz und eine gesteigerte Widerstandsfähigkeit gegen Terrorismus

Als Folgemaßnahme zur Annahme des von der Kommission vorgelegten **Aktionsplans für einen besseren Schutz des öffentlichen Raums**²⁹ fand das erste Treffen des High Risk Security Network am 14. und 15. November 2017 statt. Die mit dem Schutz von in hohem Maße gefährdeten Stätten beauftragte spanische Guardia Civil richtete diese erste Konferenz in ihrem Hauptquartier in Logroño aus. Dieses neue Netzwerk soll der Entwicklung neuer Taktiken für einen besseren Schutz von in hohem Maße gefährdeten öffentlichen Räumen Vorschub leisten. Darüber hinaus wird das erste Treffen des Betreiberforums in Brüssel am 20. Dezember 2017 stattfinden, an das sich am 21. Dezember 2017 ein spezielles Thementreffen zur Fahrzeugvermietung unmittelbar anschließen wird. Vorbereitungen für ein Treffen mit Bürgermeisterinnen und Bürgermeistern europäischer Städte wurden in Angriff genommen, das zusammen mit dem Ausschuss der Regionen im kommenden Frühjahr stattfinden soll.

In Reaktion auf eine erhöhte Gefährdungslage im Personenbeförderungs- und Gütertransportwesen und hierbei insbesondere Schienennetze haben einzelne Mitgliedstaaten ihre Sicherheitsmaßnahmen zum Schutz des Bahnverkehrs verschärft. Die Durchführung dieser Maßnahmen erfolgte dabei in fragmentierter Weise, was ein Schlaglicht auf den Bedarf nach verbesserter Koordination auf dem Gebiet der Sicherheit im Schienenverkehr wirft. Die Kommission hat daher in ihrem Arbeitsprogramm 2018 ihre Absicht bekundet, weiteren Maßnahmen zur Verbesserung der **Sicherheit von Bahnreisenden** zuzuarbeiten.

Auf dem Gebiet der Forschung wurde die Veranstaltung **Gefahrenabwehrforschung 2017** gemeinsam von der Europäischen Kommission und der estnischen Präsidentschaft in Tallinn am 14. und 15. November 2017 organisiert. Es bestand weithin Übereinstimmung darüber, dass es zusätzlicher Anstrengungen bedarf, um die Lücke zwischen Forschungsergebnissen und wirksamen Produkten und Dienstleistungen zu schließen, die sich zum Vorgehen gegen verschiedenartigen Bedrohungen der Sicherheit wie Terrorismus, Cyber-Kriminalität und Naturkatastrophen einsetzen lassen. Die Einbindung der Industrie, der akademischen Welt, von Behörden und Praktikern in einen gemeinsamen Schaffungsprozess wäre dabei hilfreich, die Anbieterseite (Industrie) und die Nachfrageseite (Endanwender) zur Konsolidierung künftiger Anforderungen und zur Herstellung von Übereinkunft über mögliche Lösungen zusammenzubringen, die eine praktische Auswirkung haben und die Arbeit von Sicherheitsexperten in naher Zukunft erleichtern können. Die Kommission wird prüfen, wie sich diese Gedanken in die Praxis umsetzen lassen.

2. Vorgehen gegen die zur Unterstützung des Terrorismus eingesetzten Mittel

Fortgeführt wurden Diskussionen mit Legislativorganen über den Vorschlag der Kommission zu Verbesserungen der **Vierten Geldwäscherichtlinie**, die bei der Bekämpfung der

²⁹ COM(2017) 612 final vom 18.10.2017.

Terrorismusfinanzierung von Nutzen sein werden. Wiederum appelliert die Kommission an die Legislativorgane, die Verhandlungen über die Gesetzgebung zu diesem vorrangigen Dossier rasch zu einem Abschluss zu führen und sich auf einen Kompromiss zu einigen, der den derzeitigen Satz an Rechtsvorschriften der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung unter anderem durch eine erhöhte Transparenz von Angaben zum wirtschaftlichen Eigentum erweitert.

Daneben wird der Vorschlag für eine **Richtlinie zur Harmonisierung der Definition des Straftatbestands der Geldwäsche und der diesbezüglichen strafrechtlichen Sanktionen**³⁰ einen Beitrag zur Überwindung von Hindernissen für die grenzüberschreitende Zusammenarbeit bei der Bekämpfung von Geldwäsche leisten. Einigung über eine allgemeine Ausrichtung wurde im Rat am 8. Juni 2017 erzielt. Sobald das Europäische Parlament seine Position am 11. Dezember 2017 verabschiedet haben wird, können bald darauf die Gespräche auf interinstitutioneller Ebene mit Blick auf die Erzielung einer Übereinkunft in der ersten Jahreshälfte 2018 aufgenommen werden.

Die Bemühungen um einen verbesserten Zugang von Strafverfolgungsbehörden über Landesgrenzen hinweg auf maßgebliche Finanzdaten, welche notwendige Hinweise auf terroristische Tätigkeiten liefern könnten, werden wie im Arbeitsprogramm der Kommission 2017 angekündigt fortgesetzt. Am 20. November 2017 hat die Kommission ein Treffen mit hochrangigen Interessenträgern aus Mitgliedstaaten und EU-Einrichtungen veranstaltet, um den Bedarf nach **zusätzlichen Maßnahmen zur Erleichterung eines grenzüberschreitenden Zugangs zu Finanzdaten zu Zwecken der Terrorismusbekämpfung** zu ermitteln. Bei diesem Treffen merkten die Mitgliedstaaten an, dass die verschiedenen Maßnahmen – ganz gleich, ob diese bereits existierten, sich in Vorbereitung oder in Planung befanden – die erforderlichen Instrumente und Lösungen bereitstellten, insbesondere die **Europäische Ermittlungsanordnung**³¹, die **Geldwäscherichtlinie**³² (einschließlich des derzeit verhandelten Änderungsvorschlags³³) und eine bevorstehende Aufforderung zur Einreichung von Vorschlägen zur Unterstützung von Projekten zur Bekämpfung der Terrorismusfinanzierung³⁴.

Der Entwurf zu einer überarbeiteten Vierten Geldwäscherichtlinie sieht die verpflichtende Schaffung **einzelstaatlicher zentralisierter Bankkontenregister und diesbezüglicher Abfragesysteme** vor, auf die die Zentralstellen für Geldwäsche-Verdachtsanzeigen zugreifen könnten. Die Kommission beurteilt derzeit die Auswirkung in Frage kommender Strategieoptionen im Hinblick darauf, im Frühjahr 2018 eine Richtlinie vorzuschlagen, die Strafverfolgungsbehörden und Vermögensabschöpfungsstellen Zugang zu den Registern und Datenabfragesystemen im eigenen Mitgliedstaat eröffnete.

Die Kommission ist daneben mit Initiativen zur Verbesserung der **Zusammenarbeit unter den zentralen Meldestellen** sowie von deren Zusammenarbeit mit den Strafverfolgungsbehörden befasst. Auch diese Arbeiten sollten bis zum Frühjahr 2018 zum Abschluss gelangen. Parallel dazu und im Hinblick auf die Vorbereitung der erforderlichen Initiativen zur Erleichterung des grenzüberschreitenden Zugangs zu Finanzdaten für

³⁰ COM(2016) 826 final vom 21.12.2016.

³¹ Richtlinie (EU) 2014/41 vom 3.4.2014.

³² Richtlinie (EU) 2015/849 vom 20.5.2015.

³³ COM(2016) 450 final vom 5.7.2016.

³⁴ http://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/home/call-fiche/isfp-call-fiche-2017-ag-terfin_en.pdf (in englischer Sprache)

Strafverfolgungsbehörden wird die Kommission weiterhin die Notwendigkeit, die technische Machbarkeit und die Verhältnismäßigkeit jedweder zusätzlicher Maßnahmen prüfen.

Die Kommission hat heute einen Bericht über die Evaluierung der Verordnung (EU) Nr. 258/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 über die **Einführung von Ausfuhrgenehmigungen für Feuerwaffen sowie von Maßnahmen betreffend deren Einfuhr und Durchfuhr** angenommen. Die Autoren gelangen darin zu dem Schluss, dass es der Verordnung weiterhin bedarf, deren Wirksamkeit jedoch durch die unzureichende Genauigkeit einzelner der darin enthaltenen Bestimmungen sowie ein kompliziertes Wechselspiel mit anderen Instrumenten des EU-Rechts eingeschränkt ist. Zum Meinungsaustausch über diese Schlussfolgerungen ist Ende Januar 2018 ein Treffen zwischen der Kommission mit Sachverständigen aus den einzelnen Mitgliedstaaten vorgesehen. Die Kommission wird ferner mehrere Treffen einberufen, um bei einer Reihe von anstehenden Herausforderungen (Beschlagnahmestatistiken, Ballistik, Zusammenarbeit mit den Ländern des westlichen Balkans) zu Fortschritten zu gelangen.

Am 18. Oktober 2017 hat die Kommission eine **Empfehlung über unmittelbare Maßnahmen** herausgegeben, **um dem Missbrauch von Ausgangsstoffen für Explosivstoffe vorzubeugen**, in der die Mitgliedstaaten dazu aufgefordert werden, für einen verstärkten Schutz gegen die Verwendung selbst hergestellter Sprengkörper zu terroristischen Zwecken umgehend eine Reihe von Maßnahmen zu ergreifen, und mit der die Zielsetzungen der Verordnung (EU) Nr. 98/2013 des Europäischen Parlaments und des Rates vom 15. Januar 2013 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe unterstützt werden. Bei einem Treffen des ständigen Sachverständigenausschusses für Ausgangsstoffe von Explosivstoffen am 12. und am 13. Dezember 2017 wird eine Bestandsaufnahme der von den Mitgliedstaaten bei der Umsetzung der Empfehlung erzielten Fortschritte erfolgen. Am 6. Dezember 2017 beschloss die Kommission, das gegen Frankreich wegen Nichterfüllung der Verordnung Nr. 98/2013 eingeleitete Vertragsverletzungsverfahren einzustellen, nachdem Frankreich die Kommission von der vollumfänglichen Umsetzung der Verordnung unterrichtet hatte. Parallel dazu ist die Kommission mit der **Überarbeitung der Verordnung (EU) Nr. 98/2013** befasst, die auf eine Verschärfung der Beschränkungen und Kontrollen in Bezug auf den Verkauf, den Besitz, die Einführung und Verwendung von Ausgangssubstanzen für Explosivstoffe abzielt und mit der die Fähigkeit der Wirtschaftsteilnehmer und der zuständigen Stellen und Strafverfolgungsbehörden der Mitgliedstaaten gestärkt werden soll, Missbrauchsfälle aufzudecken und solchen vorzubeugen; ferner soll sie dazu beitragen, zu einer größeren Einheitlichkeit der Anwendung der Verordnung unter den Mitgliedstaaten zu gelangen. Die Folgenabschätzung hinsichtlich der verschiedenen Optionen bei der Überarbeitung der Verordnung wird im Frühjahr 2018 abgeschlossen sein.

3. *Cybersicherheit und Strafjustiz im Cyberspace*

In den Schlussfolgerungen des Europäischen Rates vom 19. Oktober 2017³⁵ wurden den Initiativen des **Pakets zur Cybersicherheit**³⁶ Anerkennung gezollt. Am 20. November 2017 hat der Rat Schlussfolgerungen zur gemeinsamen Erklärung des Europäischen Parlaments und des Rates *„Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU*

³⁵ <http://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf> (in englischer Sprache)

³⁶ <https://ec.europa.eu/digital-single-market/en/policies/cybersecurity> (in englischer Sprache)

wirksam erhöhen³⁷ angenommen. Ein Aktionsplan zur Umsetzung dieser Ratsbeschlüsse soll am 12. Dezember 2017 vom Rat (Allgemeine Angelegenheiten) angenommen werden.

Die Erörterungen mit dem Rat über den vorgeschlagenen „**Rechtsakt zur Cybersicherheit**“ (der sich auf das neue Mandat der ENISA und den Zertifizierungsrahmen erstreckt)³⁸ haben begonnen. Der **Legislativvorschlag über unbare Zahlungsmittel** ist dem Europäischen Parlament und dem Rat vorgelegt worden und wird derzeit geprüft. Die Kommission fordert dringend dazu auf, nachdem die Ernennung des Berichterstatters am 13. November 2017 erfolgt ist, die Arbeit im Europäischen Parlament nunmehr in Angriff zu nehmen. Mit Bezug auf die Umsetzung der NIS-Richtlinie³⁹ fand am 28. November ein Treffen der Kooperationsgruppe statt. Die Gruppe nahm zwei ihrer Arbeitsergebnisse an, die zentrale Aspekte der Richtlinie betreffen: Leitlinien für die Ermittlung von Betreibern wesentlicher Dienste⁴⁰ im Hinblick auf bewährte Verfahren bezüglich der Kriterien, welche die Kritizität eines Betreibers definieren, und Richtlinien über Sicherheitsmaßnahmen, die einen Überblick über Referenzwerte für Messungen liefern, die bei der Absicherung von Netzwerken und Informationssystemen heranzuziehen sind⁴¹. Ein drittes Arbeitsergebnis zu Meldepflichten, in denen die Umstände dargelegt sind, unter denen Betreiber wesentlicher Dienste zur Meldung eines Vorfalls verpflichtet sein werden, wird voraussichtlich bald im schriftlichen Verfahren angenommen werden. Die Gruppe hat Gespräche über ihr erstes Arbeitsprogramm (2018-2020) aufgenommen, dessen Annahme bis Februar 2018 erwartet wird.

Die Kommission hat im 11. Fortschrittsbericht zur Sicherheitsunion⁴² zugesichert, den Bedarf nach zusätzlichen Ressourcen für Europol (insbesondere das Europäische Zentrum zur Bekämpfung der Cyberkriminalität, EC3) zu prüfen, die EC3 in die Lage versetzten, den Mitgliedstaaten Hilfestellung bei der Bewältigung von sich in Zusammenhang mit **Verschlüsselung bei strafrechtlichen Ermittlungen** stellenden Herausforderungen Unterstützung zu leisten. Bei der Betrachtung der durch die Bereitstellung einer EU-weit verfügbaren Kapazität geschaffenen Rationalisierungseffekte (gegenüber Einzellösungen auf einzelstaatlicher Ebene) hat die Kommission daneben vom Bedarf nach weitergehender Unterstützung in diesem Bereich Kenntnis genommen, wie sie am 7. und 8. Dezember 2017 vom Rat (Justiz und Inneres) gefordert worden war. Die Einschätzung des spezifischen Bedarfs nach zusätzlichen Ressourcen ist noch im Gange, und die Kommission wird im nächsten Fortschrittsbericht zur Sicherheitsunion über die hierfür bereitgestellten Mittel berichten. Die Befähigung der Strafverfolgungsbehörden aus den Mitgliedstaaten, das von EC3 bereitgestellte Instrumentarium in einem sich rasch wandelnden Umfeld zu nutzen, wird die Voraussetzungen für eine Maximierung des Investitionsnutzens schaffen und zugleich sicherstellen, dass die EU-weit verfügbaren Kapazitäten mit den Herausforderungen Schritt halten, ohne hierzu Verschlüsselung zu verbieten, einzuschränken oder aufzuweichen.

³⁷ JOIN(2017) 450 final vom 13.9.2017.

³⁸ COM(2017) 477 final/2 vom 4.10.2017.

³⁹ Richtlinie (EU) 2016/1148 vom 6.7.2016.

⁴⁰ „Sharing of good practices related to the criteria defining the criticality of an operator pursuant to Article 5(2) of the directive by means of guidelines“ (Gemeinsame Nutzung bewährter Verfahren in Bezug auf die Kriterien für die Ermittlung der Kritikalität eines Betreibers gemäß Artikel 5 Absatz 2 der Richtlinie im Wege von Leitlinien).

⁴¹ „Reference document on security measures for Operators of Essential Services“ (Bezugsdokument zu Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste).

⁴² COM(2017) 608 final vom 18.10.2017.

Bei der Tagung des Rates (Justiz und Inneres) am 7. und 8. Dezember 2017 haben die Mitgliedstaaten beschlossen, Gespräche auf Sachverständigenebene im Hinblick darauf fortzuführen, zu einer gemeinsamen Linie in Sachen möglicher Lösungen zur **Vorratsdatenspeicherung** zu finden, die den Vorgaben des Urteils vom 21. Dezember 2016 im von Tele2 Sverige AB angestregten Verfahren genügen. Die Kommission wird den Mitgliedstaaten bei diesem Prozess weiterhin Unterstützung leisten. Die Kommission erachtet diesen Prozess als Teil ihrer eigenen Abschätzung der sich aus dem Urteil ergebenden Folgen sowie ihrer laufenden Arbeiten zur Fertigstellung ihrer Handlungsempfehlungen zur weiteren Vorgehensweise in Sachen Vorratsdatenspeicherung, die im Arbeitsprogramm der Kommission für 2018 angekündigt worden war.

Wie bereits angekündigt, erwägt die Kommission, Anfang 2018 eine Gesetzesinitiative zu **elektronischen Beweismitteln** vorzulegen, die Strafverfolgungsbehörden einen Zugang zu elektronischen Beweismitteln eröffnet, welche sich in einem anderen Mitgliedstaat befinden.

4. Bekämpfung der Radikalisierung

In der Zeit seit dem jüngsten Fortschrittsbericht zur Sicherheitsunion hat die Kommission ihre Anstrengung zur Bekämpfung der Radikalisierung sowohl online als auch offline fortgeführt.

Die im Juli 2017 eingerichtete **hochrangige Expertengruppe zum Thema Radikalisierung** führte in hohem Tempo ihre Arbeit zur Erstellung ihres ersten Zwischenberichts fort, der am 24. November 2017 die Zustimmung der Mitglieder der Gruppe fand. In den vorläufigen Erkenntnissen und Empfehlungen der Gruppe ist eine Anzahl vorrangiger Themen und übergreifender Fragen benannt wie die Radikalisierung in Haft, Koordinationslösungen auf lokaler Ebene im Falle mehrerer zuständiger Behörden, Gewinn neuer Erkenntnisse zu Wegen zur Radikalisierung, Mechanismen und Strukturen der Zusammenarbeit, Bildung und soziale Inklusion sowie die externe Dimension der Bemühungen, einer Radikalisierung vorzubeugen. Die Kommission wird im nächsten Fortschrittsbericht zur Sicherheitsunion ihre Auffassung darlegen.

Das dritte Ministertreffen des **EU-Internetforums** fand am 6. Dezember 2017 statt; es führte Mitgliedstaaten, Internet-Unternehmen, Europol und Vertreter aus Wissenschaft und Zivilgesellschaft zusammen.⁴³ Bei dem Treffen wurden die Fortschritte beurteilt, die sich beim Aktionsplan gegen Terror propagierende Online-Inhalte haben verzeichnen lassen; thematisiert wurden in diesem Zusammenhang die automatische Erkennung solcher Inhalte, Verbesserungen an der „Hashes-Datenbank“ der Unternehmen als Beitrag zur Eindämmung der Verbreitung terrorpropagandistischer Inhalte, verbesserte Hinweise sowie die Ermächtigung der Zivilgesellschaft zur Stärkung der Rolle alternativer Lesarten zu Terrorpropaganda. Internet-Unternehmen berichteten, dass die beim EU-Internetforum 2016 angekündigte und 2017 eingerichtete Datenbank bekannter Online-Inhalte, die Terror propagieren (die „Hashes-Datenbank“), ihren Betrieb aufgenommen hat und bislang mehr als 40 000 Hashes bekannter terrorpropagandistischer Videos und Bilder darin erfasst worden sind. Das Potenzial dieses Instruments sollte nunmehr voll ausgeschöpft werden, und die Daten zu einer Reihe von Löschungen, die von der „Hashes-Datenbank“ angestoßen wurden, sollten ebenso wie Angaben zur Geschwindigkeit, mit der diese Löschvorgänge erfolgen, den Mitgliedern des EU-Internetforums regelmäßig zur Verfügung gestellt werden. Die Zahl manueller Hinweise, beispielsweise seitens der EU-Meldestelle für Internetinhalte, wächst ebenfalls weiter an, und die Unternehmen wurden dringend aufgefordert, sowohl die

⁴³ http://europa.eu/rapid/press-release_IP-17-5105_de.htm

Geschwindigkeit, mit der die Löschungen vorgenommen werden, als auch die Regelmäßigkeit der Berichterstattung an das EU-Internetforum zu verbessern. Internet-Plattformen berichteten, dass sie bei der Erkennung von terrorpropagandistischen Inhalten in zunehmendem Maße auf automatische Instrumente vertrauen.⁴⁴ Ebenso ist es wichtig, die Transparenz, Konsistenz und Regelmäßigkeit der Ergebnisberichterstattung zu steigern. Alle Internet-Unternehmen müssen sich an diesen gemeinsamen Bemühungen beteiligen und maßgebliche Informationen über die Löschung von Inhalten plattformübergreifend mitteilen, wobei das Ansprechen und Einbinden neuer und kleiner Unternehmen, die bislang nicht hieran beteiligt sind, im Vordergrund zu stehen hat.

Die Ergebnisse des EU-Internetforums werden daneben Informationen für die weitergehende politische Arbeit über illegale Online-Inhalte liefern, wobei die Kommission angekündigt hat, dass sie weiterhin die Zusammenarbeit mit Social-Media-Unternehmen zur Ermittlung und Entfernung terrorpropagandistischer und anderweitiger rechtswidriger Online-Inhalte suchen und erforderlichenfalls gesetzgeberische Maßnahmen zur Entfernung Terrorismus verherrlichender Inhalte vorschlagen wird.⁴⁵

5. Außendimension

Am 7. Dezember 2017 erteilte der Rat (Justiz und Inneres) der Kommission grünes Licht für die Aufnahme von Verhandlungen über ein Abkommen zwischen Kanada und der EU über die Übermittlung und Nutzung von Fluggastdatensätzen, um der Stellungnahme 1/15 des Europäischen Gerichtshofs über das zuvor angestrebte PNR-Abkommen zwischen der EU und Kanada nachzukommen. Die förmlichen Verhandlungen werden beginnen, sobald Kanada seinerseits sein Verhandlungsmandat erlangt haben wird.

Wie im Fortschrittsbericht zur Sicherheitsunion vom Oktober angekündigt will die Kommission bis zum Jahresende daneben Empfehlungen an den Rat annehmen, welche die Aufnahme von Verhandlungen über Einzelabkommen zwischen der EU und Algerien, Ägypten, Israel, Jordanien, dem Libanon, Marokko, Tunesien und der Türkei über den **Austausch personenbezogener Daten zwischen Europol und den zuständigen Behörden der vorgenannten Länder** zur Bekämpfung von Schwerekriminalität und Terrorismus zum Gegenstand haben. 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.

Was die Zusammenarbeit mit internationalen Partnern anbelangt, haben die **EU und die USA** am 17. November ein **Treffen der Minister für Justiz und Inneres** veranstaltet. Im Mittelpunkt der Begegnung standen die transatlantische Zusammenarbeit bei der Terrorismusbekämpfung, die Abwendung von Gefahren durch Cyberkriminalität und die Zusammenarbeit bei der Bekämpfung des Drogenschmuggels. Bei den Erörterungen zum Thema Terrorismusbekämpfung ging es konkret um die Bedeutung einer operativen Zusammenarbeit und eines wirksamen Informationsaustauschs. Beide Seiten hoben die Bedeutung der Erfassung, Auswertung und gemeinsamen Nutzung von Fluggastdatensätzen

⁴⁴ Der Nachrichtendienst Twitter berichtete, dass drei Viertel der zwischen Januar und Juni 2017 entfernten 300 000 Konten gelöscht wurden, noch ehe Inhalte darüber verbreitet werden konnten. Nach Angaben von YouTube wurden seit Juni 2017 mehr als 150 000 Videos entfernt. Sobald Facebook Kenntnis von terrorpropagandistischen Inhalten erlangt, werden 83 % der im Anschluss hochgeladenen Kopien innerhalb einer Stunde nach dem jeweiligen Upload vom Unternehmen entfernt.

⁴⁵ COM(2017) 650 final vom 24.10.2017.

hervor. Im Rahmen der Gespräche wurden auch die Fortschritte bei der Umsetzung gemeinsamer Maßnahmen zur Abwehr der vom Terrorismus ausgehenden Bedrohungen für die Luftfahrt und zur Anhebung der allgemeinen Messlatte für die Luftverkehrssicherheit erörtert. Die EU und die USA verwiesen auf ihre Maßnahmen zur Bekämpfung der Terrorismusfinanzierung und der Geldwäsche unter anderem in Gestalt gemeinsam unternommener Arbeiten und Tätigkeiten innerhalb der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“. Im Hinblick auf den Missbrauch des Internet für terroristische Zwecke stimmten die Gesprächspartner darin überein, dass Handlungsbedarf besteht, der die Beteiligung einer Vielzahl an Interessenpartnern, darunter auch des privaten Sektors und der Zivilgesellschaft, erfordert. Das nächste Treffen der Minister für Justiz und Inneres der EU und der USA soll im Mai 2018 in Sofia stattfinden.

Was die Luftverkehrssicherheit anbelangt, treffen sich die Europäische Kommission und weitere EU-Dienststellen regelmäßig mit Vertretern der Mitgliedstaaten, um Einigung über einen **integrierten Ansatz zur verstärkten und vorrangigen Verfolgung von Bemühungen um den Aufbau von Kapazitäten in Drittstaaten** herzustellen. Zu den vorgeschlagenen Maßnahmen zählen Fortbildungs- und Übungsveranstaltungen unter anderem zu den Themen Sicherheitskultur, Zugangskontrolle, Sichtungsverfahren und Zertifizierung von Auditoren. Dabei werden gesonderte Treffen zu jedem der untersuchten Drittstaaten veranstaltet, um zu jedem dieser Staaten präzise Maßnahmen zu konzipieren.

Als Folgemaßnahme zur gemeinsamen Erklärung über die **strategische Partnerschaft zwischen der NATO und der EU** hat der Rat am 5. Dezember einen zweiten Durchführungsbericht angenommen.⁴⁶ In diesem Bericht werden die Kernbereiche umrissen, in denen Fortschritte verzeichnet worden sind, einschließlich Cybersicherheit und das Vorgehen gegen hybride Bedrohungen. Im September und Oktober 2017 haben die EU und die NATO erstmals eine parallele und koordinierte Übung (EU PACE17/CMX17) durchgeführt, der ein hybrides Bedrohungsszenario zugrunde lag. Zusammen mit dem Bericht wurde ein Bündel von 24 zusätzlichen Vorschlägen für eine weitere Intensivierung und Vertiefung der Zusammenarbeit zwischen EU und NATO angenommen. Die neuen Vorschläge erfassen alle sieben in der gemeinsamen Warschauer Erklärung benannten Bereiche der Zusammenarbeit: Vorgehen gegen hybride Bedrohungen; Ausweitung der operativen Zusammenarbeit, auch auf See und im Bereich der Migration; Cybersicherheit und Gefahrenabwehr; Verteidigungsfähigkeit; Rüstungsindustrie und -forschung; Übungen; Aufbau von Kapazitäten in den Bereichen Verteidigung und Sicherheit sowie politischer Dialog. Mehrere der Vorschläge zielen auf eine verstärkte Zusammenarbeit auf den Gebieten der Terrorismusbekämpfung. So soll im ersten Halbjahr 2018 gemeinsam ein informeller Workshop veranstaltet werden, um zu einem gemeinsamen Verständnis dabei zu gelangen, inwiefern die Entwicklung von Verteidigungskapazitäten den zur Terrorismusbekämpfung unternommenen Anstrengungen zugutekommen kann. Aufbauend auf den bei der 2017 durchgeführten Übung gemachten Erfahrungen und gewonnenen Erkenntnissen wird ein Plan zur Einführung paralleler und untereinander koordinierter Übungen zwischen der EU und der NATO in den Jahren 2019-2020 entwickelt werden. Darüber hinaus werden ab 2018 gemeinsame Fortbildungs- und Übungsmodulare eingeführt werden.

⁴⁶ Dem durch die Minister beider Organisationen erteilten Auftrag entsprechend, alle zwei Jahre Bericht zu erstatten, wurde der erste Fortschrittsbericht über die Umsetzung der Vorschläge dem jeweiligen Rat im Juni 2017 vorgelegt. Der zweite Fortschrittsbericht beleuchtet den Zeitraum Juli bis Dezember 2017.

IV. SCHLUSSBEMERKUNGEN

In diesem Bericht wird eine Reihe von Maßnahmen dargelegt, die auf EU-Ebene zur Intensivierung des Informationsaustauschs zur Stärkung der inneren Sicherheit und für ein besseres Außengrenzenmanagement unternommen werden. Die vorgeschlagene Verordnung zur Interoperabilität schafft die Voraussetzungen für eine zielgerichtete und intelligente bestmögliche Nutzung vorhandener Daten sowie für die Berücksichtigung des Prinzips eines Datenschutzes durch Technikgestaltung („data protection by design“). Die einzelstaatlichen Behörden sollen dabei unterstützt werden, wirksamer gegen grenzübergreifende Bedrohungen vorzugehen und über Landesgrenzen hinweg agierende Terroristen besser aufzuspüren. Damit markiert die Verordnung einen grundlegenden Wandel in Bezug auf das EU-Datenmanagement auf dem Gebiet der Sicherheit und der Außengrenzen.

Die Annahme des nächsten Berichts über die beim Aufbau einer wirksamen und echten Sicherheitsunion erzielten Fortschritte ist für Januar 2018 vorgesehen.