HEINRICH BÖLL STIFTUNG

Die Grünen | EFA
im Europäischen Parlament

Grenzwertig

Eine Analyse der neuen EU-Grenzüberwachungsinitiativen EUROSUR und "intelligente Grenzen"

Eine Studie der Heinrich Böll Stiftung

Von
Dr. Ben Hayes
Mathias Vermeulen

Juni 2012

Heinrich-Böll-Stiftung
Die grüne politische Stiftung
Schumannstraße 8 10117 Berlin
Telefon +49 (0)30 285 34-0
www.boell.de

Ska Keller
Abgeordnete des Europaparlaments, Grüne/EFA
Europäisches Parlament, Rue Wiertz 60, B-1047 Brüssel
Telefon: +32 (0)2 28 45379
E-Mail: franziska.keller@europarl.europa.eu

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

AIS	Automatische Identifikationssysteme
CISE	Gemeinsamer Informationsraum
EBF	Europäischer Außengrenzenfonds
EKPN	Europäisches Küstenpatrouillennetz
EuGH	Europäischer Gerichtshof
EDSB	Europäischer Datenschutzbeauftragter
EES	Einreise-/Ausreisesystem
EMSA	Europäische Agentur für die Sicherheit des Seeverkehrs
EPSF	Europäisches Programm für Sicherheitsforschung
EUROSUR	Europäisches Grenzkontrollsystem
FRONTEX	Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union
FSC	FRONTEX Situation Centre
GMES	Globale Umwelt- und Sicherheitsüberwachung
ISF	Fonds für innere Sicherheit
LRIT	Fernidentifizierung und -verfolgung
NKZ	Nationales Koordinierungszentrum
RTP	Registrierungsprogramm für Reisende
SBI-net	Secure Border Initiative Network (Netzwerkinitiative zur Grenzsicherung)
SIS	Schengener Informationssystem
DSA	Drittstaatenangehörige/-r
VIS	Visa-Informationssystem
VMS	Schiffsüberwachungssysteme
VDS	Schiffsortungssystem

Vorwort

Die Umbrüche in Nordafrika haben kurzfristig zu einem leichten Anstieg Flüchtender nach Europa geführt. Es hat nachweislich jedoch nie eine „Flüchtlingswelle“ nach Europa gegeben. Mit Abstand die meisten Flüchtlinge sind in den arabischen Nachbarländern aufgenommen worden. Gleichwohl haben die Staats- und Regierungschefinnen und -chefs der Europäischen Union in vorschneller Reaktion im Juni 2011 einen weitreichenden Beschluss gefasst, der auf eine neue Form der Grenzsicherungspolitik der EU zum „Schutz“ vor Migration hinausläuft. Neben neuen Regelungen für die Wiedereinführung von Grenzkontrollen innerhalb des Schengen-Raums drängen die Staats- und Regierungschefinnen und -chefs auch auf eine Aufrüstung der EU-Außengrenzen mit modernster Überwachungstechnologie. Die EU soll zu einer elektronischen Festung ausgebaut werden.

Der Beschluss der Regierungsvertreter/-innen sieht zum einen den raschen Aufbau des neuen Europäischen Überwachungssystems EUROSUR vor. Dabei geht es neben einer stärkeren Kooperation der europäischen Grenzschutzbehörden auch um die Überwachung der EU-Außengrenzen mit modernster Überwachungstechnologie durch die europäische Grenzschutzagentur FRONTEX. Selbst Drohnen sollen künftig über dem Mittelmeer und den nordafrikanischen Küsten kreisen. Ziel des High-Tech-Einsatzes ist es, Flüchtlingsboote zu entdecken und zu stoppen, ehe sie die europäischen Grenzen überhaupt erreichen. Der Legislativvorschlag zu EUROSUR liegt mittlerweile vor und wird derzeit im Rat und im Europäischen Parlament beraten.

Zum anderen drängen die Mitgliedstaaten auf die Einführung sogenannter „Smart Borders“ („intelligente Grenzen“). Damit soll die Totalüberwachung von Reisebewegungen an den europäischen Grenzübergängen geschaffen werden. Geplant ist die Einführung einer Mega-Ausländerdatenbank nach US-Vorbild, in der sich alle Nicht-EU-Bürger/-innen mit Fingerabdrücken registrieren müssen, wenn sie in die EU ein- und ausreisen. Damit sollen sogenannte „Overstayer“ („Überzieher/-innen“) identifiziert werden. Das sind Drittstaatenangehörige, die länger in der EU bleiben, als es ihr Visum für eine befristete Aufenthaltsdauer erlaubt. In den USA ist das System gescheitert; die Ausreisekontrollen wurden nie flächendeckend eingeführt. In der EU soll es nach dem Willen der Staats- und Regierungsvertreter/-innen trotzdem kommen – koste es, was es wolle (die EU-Kommission rechnet mit bis zu 1,1 Milliarden Euro). Den Gesetzesvorschlag zu „Smart Borders“ will sie auf Drängen der Mitgliedstaaten im Sommer 2012 vorlegen.

EUROSUR und „Smart Borders“ sind die zynische Antwort der EU auf den Arabischen Frühling. Sie stehen für eine neue Form der europäischen Grenzsicherungspolitik, mit der sich die EU zunehmend nach außen (und über Binnenkontrollen im Schengen-Raum auch nach innen) gegen Flüchtlinge und Migrant/-innen abschottet. Manche Innenminister/-innen nehmen dafür selbst Verletzungen von Grundrechten in Kauf.

Die vorliegende Studie von Ben Hayes und Mathias Vermeulen macht deutlich, dass EUROSUR einer Politik der EU Vorschub leistet, bei der die Rechte auf Asyl und Schutz nicht mehr gewährleistet sind. FRONTEX steht seit langem in der Kritik für seine sogenannten „Push-Back“-Operationen, bei denen Flüchtlingsboote abgefangen und zurück an ihren Ausgangshafen eskortiert werden. Italien wurde im Februar 2012 vom Europäischen Gerichtshof für Menschenrechte wegen solcher Operationen verurteilt, weil die italienischen Grenzschützer/-innen unterschiedslos alle Flüchtlinge eines

abgefangenen Bootes nach Libyen zurückgeschickt haben – auch Flüchtlinge, die ein Recht auf Asyl und internationalen Schutz gehabt hätten. Die mit EUROSUR geplante Überwachung des Mittelmeerraums durch Drohnen, Satelliten und Schiffsüberwachungssysteme wird es künftig einfacher machen, die Boote zu entdecken. Die im Rahmen von EUROSUR ebenfalls geplante Kooperation mit Drittstaaten und vor allem mit den nordafrikanischen Mittelmeeranrainerländern wird, so steht zu befürchten, den Weg ebnen für eine Ausweitung der „Push-Back"-Operationen.

Die EU-Kommission kündigt EUROSUR freilich positiv an: Die geplante Überwachung des Mittelmeerraums mit Drohnen, Satelliten und Schiffsüberwachungssystemen werde helfen, mehr schiffsbrüchige Flüchtlinge auf offener See zu retten. Die vorliegende Studie verdeutlicht, wie wenig Substanz hinter dieser Schönfärberei steckt. Seenotrettungseinheiten sind gerade nicht in EUROSUR und den Informationsaustausch der Grenzschützer/-innen eingebunden. Dabei wäre gerade das wichtig. Der erst jüngst veröffentlichte Bericht des Europarats zum Tod von 63 Migrant/-innen, die in ihrem seeuntüchtigen Boot verhungerten und verdursteten, kommt zu dem Schluss, dass das Problem nicht die Ortung des Bootes war, sondern ein Verantwortungsvakuum in Europa. Niemand ist den Flüchtlingen zu Hilfe geeilt – obwohl die Lage des Bootes bekannt war.

Als Reaktion auf den Arabischen Frühling drängen die Mitgliedstaaten der EU nicht nur auf eine Komplettüberwachung des Mittelmeers, sondern auch auf eine elektronische Aufrüstung an den Grenzübergängen. Damit geraten auch ganz normale Reisende ins Visier der europäischen Grenzschützer/-innen. Das Wort vom Daten-Tsunami ist da durchaus angemessen. Das EU-Programm für „intelligente Grenzen" hätte die Einrichtung einer der weltweit größten biometrischen Datenbanken zur Folge – und zwar nicht zur Bekämpfung von Terrorismus oder grenzüberschreitender Kriminalität (selbst dies wären bedenkliche Vorhaben), sondern lediglich mit dem Ziel, Einzelpersonen ausfindig zu machen, die ihre per Visum genehmigte Aufenthaltsdauer in der EU überschritten haben.

Es gehört zu den zentralen Ergebnissen der Studie, dass die neuen Grenzüberwachungsinitiativen der EU nicht nur zentrale Grundrechte verletzen, sondern trotz des fragwürdigen Nutzens auch Milliarden kosten würden – und das in Zeiten von allgegenwärtigen Haushaltskürzungen und Sparmaßnahmen. Davon profitieren vor allem die großen europäischen Rüstungskonzerne, die mit EU-Fördermitteln „smart gates", Drohnen und andere Überwachungstechnologie entwickeln. Es scheint offensichtlich, dass mit der technologischen Aufrüstung der EU-Außengrenzen ein neues Geschäftsfeld für die europäische Sicherheits- und Rüstungsindustrie geschaffen wird. Hier treffen sich Industrieinteressen mit den Zielen politischer Hardliner/-innen, die in Migration eine neue Bedrohung der inneren Sicherheit der EU sehen.

Die neuen Grenzüberwachungsinitiativen der EU sind nicht nur Sinnbilder für eine neue technologische Aufrüstung. Sie stehen auch für die politische Hilflosigkeit der EU, mit Migration und Flüchtlingen umzugehen. Von den 500.000 Menschen, die sich wegen der politischen Umbrüche in Nordafrika auf die Flucht begaben, ist nicht einmal ein Zwanzigstel nach Europa gekommen. Das Problem ist vielmehr, dass die meisten Flüchtlinge an nur wenigen Orten in Europa stranden. Nicht die EU ist überfordert, sondern die am stärksten beanspruchten lokalen Strukturen im italienischen Lampedusa, im griechischen Evros-Gebiet und auf Malta. Es ist deshalb wenig hilfreich, Migration als neues Bedrohungsszenario zu zeichnen und an den Grenzen militärische Überwachungstechnologie einzusetzen. Statt Flüchtlinge aufzunehmen, wehrt die Bundesregierung im Schulterschluss mit

anderen europäischen Regierungen seit Jahren im Europäischen Rat erfolgreich eine Neuregelung der Dublin-Verordnung ab. Flüchtlinge und Migrant/-innen sollen auch in Zukunft in dem EU-Land bleiben, in dem sie ankommen.

Die Abwehr der Mitgliedstaaten geht sogar so weit, dass die Rettung schiffsbrüchiger Flüchtlinge gefährdet ist. Bei FRONTEX-Operationen werden in Seenot geratene Flüchtlinge nicht, wie nach internationalem Recht vorgesehen, in den nächstliegenden Hafen gebracht, sondern in einen Hafen des Mitgliedstaats, der die Operation leitet. Dahinter steht die Philosophie: „Bloß nicht zu uns!“ Sie ist auch die Ursache für das vom Europarat konstatierte Verantwortungsvakuum bei der europäischen Seenotrettung. Solange die Mitgliedstaaten nicht zu mehr Solidarität und Menschlichkeit bereit sind, wird daran auch EUROSUR nichts ändern.

Was hilfreich wäre, sind bessere, europaweite Asylstandards. Die entsprechenden EU-Richtlinien werden gerade überarbeitet – allerdings unter der strikten Maßgabe, dass die Neuregelungen nicht mehr kosten als die bisherigen und dass sie nicht zu einer relativen Ausweitung der Asylanträge führen. Zynischerweise haben das die Staats- und Regierungschef/-innen in genau demselben Beschluss festgezurrt, in dem sie auch auf die rasche Einführung der milliardenschweren Überwachungsinitiativen drängten. Das Europäische Unterstützungsbüro für Asylfragen (EASO) wird dementsprechend kurz gehalten, ganz im Gegensatz zu FRONTEX, deren Budget neunmal so groß ist.

Weil die Mitgliedstaaten die eigentlichen Probleme nicht lösen wollen, rüsten sie an den Außengrenzen auf. Das ist Kirchturmpolitik im großen Maßstab. Europäische Grundwerte werden dabei zur Disposition gestellt – vermeintlich zum Schutz eigener Interessen. Das ist schon mehr als „grenzwertig“.

Berlin/Brüssel, Mai 2012

Barbara Unmüßig
Vorstand der Heinrich-Böll-Stiftung

Ska Keller
Mitglied des Europäischen Parlaments

Zusammenfassung

Die Studie „Grenzwertig“ betrachtet zwei neue EU-Initiativen zur Grenzüberwachung: die Schaffung eines „Europäischen Grenzkontrollsystems“ (EUROSUR) und die Einführung des sogenannten „Smart Borders“-Pakets, das die Schaffung eines „Einreise-/Ausreisesystems“ (EES = Entry-Exit System) und die Einführung eines „Registrierungsprogramms für Reisende“ (RTP = Registered Traveller Programme) umfasst. EUROSUR verspricht eine verbesserte Überwachung der See- und Landgrenzen der EU unter Einsatz eines riesigen Aufgebots an neuen Technologien, unter anderem Drohnen (unbemannte Luftfahrzeuge), Offshore-Sensoren und Satellitensuchsystemen. Mit dem EES sollen die Ein- und Ausreisebewegungen von Personen an den Außengrenzen des Schengen-Raums aufgezeichnet und die biometrischen Identitätskontrollen auf alle Nicht-EU-Bürger/-innen ausgeweitet werden (auch auf diejenigen, die derzeit kein Visum für die Einreise in die EU benötigen). Damit sollen die Grenzposten Personen, die ihre per Visum genehmigte Aufenthaltsdauer in der EU überzogen haben („Overstayer“ bzw. "Überzieher/-innen"), leichter ausfindig machen können. Solche biometrischen Kontrollen an allen Grenzen werden die Wartezeiten erheblich verlängern. Daher soll mit dem EES ein Registrierungsprogramm für Reisende einhergehen, welches vorab überprüften Drittstaatenangehörigen, die nach bisherigen Erkenntnissen kein Sicherheitsrisiko für die EU darstellen, eine beschleunigte Einreise ermöglichen würden. Dazu dienen automatische Kontrollgates, wie sie an einigen europäischen Flughäfen bereits installiert sind. EU-Politiker/-innen sowie die Hersteller/-innen dieser Gates hoffen, dies werde überall in der EU zur Einrichtung sogenannter „intelligenter Grenzen“ (*smart borders*) führen.

Die Vorschläge der EU aus dem Jahr 2008 haben infolge der vermeintlichen „Migrationskrise“ im Zuge des sogenannten „Arabischen Frühling“ des Jahres 2011, welche die Einreise tausender Tunesier/-innen nach Frankreich mit sich brachte, neu an Dynamik gewonnen. Jetzt treten sie in eine entscheidende Phase ein. Das Europäische Parlament und der Rat haben gerade begonnen, über den Legislativvorschlag zum EUROSUR-System zu verhandeln, und die Kommission wird voraussichtlich binnen Monaten formelle Vorschläge für die Einrichtung eines EES und RTP vorlegen.

Zusammengenommen könnten EUROSUR und das „Smart Borders“-Paket Kosten in einer Größenordnung von zwei Milliarden Euro oder mehr verursachen. Sie würden zur Erhebung biometrischer Daten von Millionen Reisenden sowie zur Installation kostspieliger neuer Grenzkontrollsysteme in den Mitgliedstaaten und bei der EU-Grenzschutzagentur FRONTEX führen. Außerdem würden sich die Wartezeiten an den EU-Außengrenzen verlängern. Die Europäische Kommission hat mehrere Folgenabschätzungen vorgenommen, konnte damit dem Bericht zufolge aber keinen dringenden gesellschaftlichen Bedarf an den neuen Systemen belegen. Die finanziellen Schätzungen der Kommission weisen eine große Fehlermarge auf und die Organe der EU haben es versäumt, die unüberwindlichen Schwierigkeiten der USA bei der Einführung vergleichbarer Systeme in ihre Überlegungen mit einzubeziehen (US VISIT, das immer noch nicht in der Lage ist, die Ausreise von Personen aus den USA zu registrieren, und SBINET, ein Grenzüberwachungssystem an der Grenze zu Mexiko, das infolge technischer Probleme und explodierender Kosten fallengelassen wurde). Die Autoren fordern eine eingehende öffentliche Debatte über den Bedarf an weiteren

kostspieligen EU-weiten Datenbanken und Überwachungssystemen in einer Zeit der lähmenden Geldknappheit.

In dem Bericht wird ferner das Verfahren zur Entscheidungsfindung kritisiert. Über die Einrichtung vergleichbarer Systeme, etwa EUROPOL und FRONTEX, wurde zumindest im Europäischen Parlament, in den Parlamenten der Mitgliedstaaten und in der Zivilgesellschaft diskutiert. Diese Vorgehensweise wurde bei EUROSUR – und eingeschränkt auch bei der Initiative zur Einrichtung „intelligenter Grenzen" – durch einen technokratischen Prozess ersetzt, der es ermöglichte, das System lange vor der nun auf dem Tisch liegenden Gesetzesvorlage zu entwickeln und erhebliche öffentliche Ausgaben dafür zu tätigen. Nach fünfjähriger technischer Entwicklung geht die Europäische Kommission nun davon aus, dass der Rechtsrahmen verabschiedet und das EUROSUR-System noch im selben Jahr (2013) – zunächst in einer „BETA"-Version – in die Praxis umgesetzt wird, und stellt damit das Europäische Parlament faktisch vor vollendete Tatsachen.

Das EUROSUR-System

Das erklärte Ziel von EUROSUR ist die Verbesserung des „Lagebewusstseins" und der Reaktionsfähigkeit der Mitgliedstaaten und der Grenzschutzagentur FRONTEX, um illegale Einwanderung und grenzüberschreitende Kriminalität an den See- und Landaußengrenzen der EU zu verhindern. In der Praxis würden die Schengen-Staaten mit dieser Verordnung verpflichtet, Land- und Seegrenzen, die in puncto illegaler Einwanderung als Hochrisikogrenzen eingestuft werden, rund um die Uhr umfassend zu überwachen. Darüber hinaus würde FRONTEX mit der Überwachung der offenen Seegebiete außerhalb des Hoheitsgebiets der EU sowie der nordafrikanischen Küsten und Häfen beauftragt. Durch ein erhöhtes Situationsbewusstsein für die Vorgänge auf hoher See sollen sich die EU-Mitgliedstaaten veranlasst sehen, in Übereinstimmung mit dem internationalen Seerecht angemessene Schritte zur Ortung und Rettung von Personen in Seenot einzuleiten. Die Kommission hat wiederholt die zukünftige Rolle von EUROSUR für den „Schutz und die Rettung" von Migrant/-innen hervorgehoben, doch weder in der vorgeschlagenen Verordnung noch in zahlreichen Bewertungen, Studien oder Forschungs- und Entwicklungsprojekten ist irgendwo definiert, wie das genau erfolgen wird. Es werden auch keinerlei Verfahren erläutert, was mit den „Geretteten" geschehen soll. Vor diesem Hintergrund und ungeachtet der humanitären Krise unter Migrant/-innen und Flüchtlingen, die auf dem Mittelmeer nach Europa unterwegs sind, stellt EUROSUR weniger ein lebensrettendes Instrument dar, sondern ergänzt vielmehr die langjährige europäische Politik, mit der diese Menschen daran gehindert werden, in das Hoheitsgebiet der EU zu gelangen (unter anderem mittels sogenannter „Zurückdrängungs"-Aktionen (*push back operations*), bei denen die Migrantenboote gezwungen werden, in das Land zurückzukehren, aus dem sie gekommen sind).

Das EUROSUR-System bedient sich umfangreicher neuer Überwachungstechnologien und 24 verschiedener einzelstaatlicher Grenzüberwachungssysteme und Koordinierungszentren, die bilateral und mittels FRONTEX vernetzt werden sollen. Doch trotz des High-Tech-Anspruchs wurde das geplante EUROSUR-System keiner angemessenen technologischen Risikobewertung unterzogen. Die Entwicklung neuer Technologien und die bilateral und durch FRONTEX zu leistende Vernetzung von 24 verschiedenen einzelstaatlichen Überwachungssystemen und Koordinierungszentren ist nicht nur hochkomplex, sondern auch äußerst kostspielig. Doch die Einzigen, die gefragt wurden, ob das ihrer Meinung nach gelingen wird, sind FRONTEX und die Unternehmen, die die Hard- und Software

verkaufen. Die Europäische Kommission schätzt, dass EUROSUR 338 Millionen Euro kosten wird, doch ihre Verfahrensweisen halten einer genaueren Überprüfung nicht stand. In Anbetracht der jüngsten Aufwendungen aus dem EU-Außengrenzenfonds, dem Forschungsrahmenprogramm und maßgeblichen Budgets für den geplanten Fonds für innere Sicherheit (mit dem die Umsetzung der EU-Strategie der inneren Sicherheit von 2014 bis 2020 unterstützt wird) könnte EUROSUR am Ende leicht das Doppelte oder Dreifache kosten: annähernd 874 Millionen Euro. Wird der Gesetzentwurf für EUROSUR bzw. den Fonds für innere Sicherheit nicht mit einer Ausgabendeckelung versehen, dann wird das Europäische Parlament keine Möglichkeit haben, eine beliebige Kostenüberschreitung zu verhindern. Abgesehen von der regelmäßigen Berichterstattung durch die Kommission und FRONTEX existiert kein einziger Mechanismus zur finanziellen Rechenschaftspflicht. Und da das Projekt aus mehreren EU-Haushaltstiteln finanziert wird, ist es schon jetzt sehr schwierig zu überwachen, was tatsächlich ausgegeben wurde.

In ihrem Legislativvorschlag behauptet die Europäische Kommission, EUROSUR werde personenbezogene Daten lediglich in „Ausnahmefällen" verarbeiten, demzufolge wird auf den Schutz der Privatsphäre und den Datenschutz kaum eingegangen. In dem Bericht wird der Einwand erhoben, dass mit dem Einsatz von Drohnen und hochauflösenden Kameras wahrscheinlich viel mehr personenbezogene Daten erhoben und verarbeitet werden als behauptet. Es sind detaillierte Datenschutzvorkehrungen erforderlich, insbesondere weil EUROSUR in den großen Gemeinsamen Informationsraum (CISE) der EU integriert werden soll, in dem Informationen mit einer ganzen Reihe dritter Akteure ausgetauscht werden können, unter anderem mit Polizeibehörden und Verteidigungskräften. Die Autoren fordern außerdem eine sachgerechte Aufsicht über EUROSUR. Die Verarbeitung personenbezogener Daten durch die nationalen EUROSUR-Koordinierungszentren sollte von den nationalen Datenschutzbehörden kontrolliert werden. Der Europäische Datenschutzbeauftragte sollte die Verarbeitung personenbezogener Daten durch FRONTEX überwachen. EUROSUR beabsichtigt auch den Informationsaustausch mit „benachbarten Drittländern" auf der Grundlage bilateraler oder multilateraler Abkommen mit Mitgliedstaaten. Im Gesetzgebungsentwurf wird ein solcher Austausch jedoch explizit ausgeschlossen, wenn Drittländer diese Informationen nutzen könnten, um Personen oder Gruppen ausfindig zu machen, die Gefahr laufen, Opfer von Folter, unmenschlicher oder erniedrigender Behandlung oder einer anderen Verletzung der Grundrechte zu werden. Die Autoren wenden ein, dass dieser Vorbehalt unmöglich Bestand haben kann, ohne dass der betreffende Datenaustausch in seiner Gesamtheit erfasst und ein geeignetes Aufsichtssystem installiert wird.

„Intelligente Grenzen" (Smart Borders)

Während das EUROSUR-System auf illegale Grenzübertritte ausgerichtet ist, dienen die Vorschläge zu „intelligenten Grenzen" der verstärkten Kontrolle von Drittstaatenangehörigen, die in die EU einreisen. Speziell mit dem Vorhaben eines Einreise-/Ausreisesystems sollen Overstayer ausfindig gemacht und verhindert werden. Dabei handelt es sich um Personen, die mit einem gültigen Reisedokument und/oder Visum legal in die EU eingereist, aber nach Ablauf ihrer gesetzlichen Aufenthaltsberechtigung zu „illegalen Migrant/-innen" geworden sind. Nach Angaben der Europäischen Kommission bilden sie die größte Gruppe „illegaler Einwanderinnen und Einwanderer" in der EU. Mit dem EES würden Ort und Zeit der Ein- und Ausreise von Drittstaatenangehörigen registriert, um ihre Ausreise zu verifizieren bzw. sie ausfindig zu machen, wenn sie ihre genehmigte Aufenthaltsdauer überschreiten. In diesem Fall würde automatisch eine Warnmeldung an die

zuständigen Behörden der Mitgliedstaaten geschickt. Mit dem EES soll eine zentralisierte europäische Datenbank aufgebaut werden, die auch biometrische Daten wie Fingerabdrücke und Gesichtsbilder *aller* in den Schengen-Raum einreisenden Drittstaatenangehörigen enthält. Eine derart umfangreiche Datenerfassung ist nur dann legal und legitim, wenn es dafür zwingende Gründe im Bereich der öffentlichen Sicherheit oder der öffentlichen Ordnung gibt. Die Autoren sind der Auffassung, dass die Europäische Kommission die Notwendigkeit einer solchen Datenerfassung nicht deutlich machen konnte.

Die Autoren führen außerdem an, dass es viele völlig legale Gründe gibt, warum Menschen ihre genehmigte Aufenthaltsdauer überziehen. Eine EES-Warnmeldung könnte daher niemals zu automatischen Sanktionen führen, sondern höchstens eine *Vermutung* des illegalen Aufenthalts begründen. Deshalb müsste daraufhin stets ein (administratives) Verfahren eingeleitet werden, um festzustellen, ob jemand ein Aufenthaltsrecht in der EU besitzt oder nicht. Somit könnte das EES bestenfalls die Grenzposten bei den Einreisekontrollen unterstützen; die Behauptungen, durch das EES würden mehr „illegale Einwanderinnen und Einwanderer" aufgespürt und zurückgeführt, entbehren jeder Grundlage. Ein weiteres Argument, das zugunsten des EES angeführt wird, ist die verbesserte Erhebung statistischer Zahlen zu typischen Reisebewegungen und Einwanderungsrouten, was der EU-Einwanderungspolitik dienlich ist. In Wirklichkeit könnten solche Daten jedoch leicht auf anonyme und sehr viel kostengünstigere Weise erhoben werden. Für diesen Zweck Unmengen an personenbezogenen Daten zu sammeln, wäre eindeutig unverhältnismäßig. Überdies fehlen auch seriöse Belege für die Wirksamkeit und Effizienz von Einreise-/Ausreisesystemen auf einzelstaatlicher Ebene und außerhalb der EU.

Für Drittstaatenangehörige hätte ein EES der EU überdies erheblich längere Wartezeiten bei der Einreise in den Schengen-Raum zur Folge. Wer ein Visum benötigt, muss bei der Einreise ohnehin schon biometrische Daten zur Verfügung stellen. Reisende aus Staaten der sogenannten „weißen Liste", die kein Vorab-Visum benötigen, sind jedoch von dieser Auflage befreit. Die Hochrechnung der Grenzübertrittsstatistiken, die im Zuge einer umfassenden Monitoring-Übung 2009 erhoben wurden, zeigt, dass dies zur Erfassung der Fingerabdrücke von jährlich weiteren 57 Millionen Bürger/-innen von Drittstaaten der „weißen Liste" führen könnte. Eine frühere Folgenabschätzung hat ergeben, dass die Erfassung biometrischer Daten den Zeitaufwand für die Einreiseformalitäten des „US VISIT"-Programms der USA um durchschnittlich 15 Sekunden erhöhte. Könnte die EU diese Zielvorgabe einhalten, dann würde das bei 57 Millionen Drittstaatenangehörigen immer noch 27 Jahre zusätzlicher Wartezeit pro Jahr an den EU-Grenzen bedeuten! Die Kommission schlägt vor, diese zusätzlichen Restriktionen für grenzüberschreitende Reisen durch die Einführung eines Registrierprogramms für Reisende „auszugleichen". Damit könnten vorab überprüfte Personen viel schneller über die Grenzen gelangen als nicht registrierte Reisende. Allerdings könnte es nach Schätzung der Kommission sein, dass von den annähernd 100 Millionen Drittstaatenangehörigen, die jedes Jahr in den Schengen-Raum einreisen, pro Jahr nur vier bis fünf Millionen Reisende tatsächlich ein RTP der EU nutzen würden. Sicherlich würde ein solches RTP Geschäftsreisenden das Leben erleichtern, doch die große Mehrheit der Reisenden hätte zweifellos nichts davon und der vorhandene Druck an den Außengrenzen des Schengen-Raums würde nicht nachlassen.

Nach Angaben der Europäischen Kommission könnten sich die Entwicklungskosten für das zentrale EES und RTP in einer Größenordnung von 400 Millionen Euro bewegen, dazu kommen

Unterhaltungskosten von jährlich 190 Millionen Euro in den ersten fünf Jahren. Obwohl es keinerlei Gesetzentwurf, ja nicht einmal eine grundsätzliche Einigung über die Einführung „intelligenter Grenzen“ in der EU gibt, hat die Kommission aus dem geplanten Fonds für innere Sicherheit der EU (2014 – 2020) bereits 1,1 Milliarden Euro für die Entwicklung des EES und RTP zugewiesen. Die explodierenden Kosten und zahlreichen Verzögerungen bei der Umsetzung des Schengener Informationssystems II (welches die anfänglich geschätzten Kosten letztendlich um das Fünffache übertraf) sollten den Entscheidungsträger/-innen der EU Warnung genug sein, dass die Einrichtung dieser Datenbanken große finanzielle Auswirkungen haben wird – gerade jetzt, wo die EU angesichts massiver Spardiktate in anderen Bereichen um ihre Legitimität ringen muss. Die Autoren der Studie halten es für unklug, dass die EU auch nur erwägt, ein weiteres groß angelegtes IT-System in Angriff zu nehmen, bevor das Visa-Informationssystem und das Schengener Informationssystem II erfolgreich umgesetzt sind. Angenommen, diese beiden Systeme erweisen sich als wirksam, dann ist es für die Kommission immer noch ein weiter Weg, den Bedarf an intelligenteren Grenzen zu belegen.

1 Einführung

Die 500 Millionen Bürger/-innen der EU bewohnen ein Gebiet, das von Landgrenzen mit insgesamt 7.400 km Länge und Küstenbereichen („Seegrenzen“) von 57.800 km Länge eingefasst ist.[1] Schätzungen zufolge reisen jedes Jahr ungefähr 300 Millionen Menschen – davon knapp 50% Nicht-EU-Bürger/-innen – in die EU ein und wieder aus.[2] Die meisten von ihnen tun dies auf rechtlich einwandfreiem Wege. Als Anfang 2011 etwa 25.000 Tunesier/-innen wegen der Umbrüche, die mit dem sogenannten Arabischen Frühling einhergingen, nach Italien flohen, gab dies für die Europäische Union den Ausschlag, die Umsetzung dreier ambitionierter Vorschläge zur Verhinderung von illegaler Einwanderung und unerlaubtem Aufenthalt voranzutreiben.[3] Diese sind: (i) die Schaffung eines „Europäischen Grenzkontrollsystems“ (EUROSUR); (ii) die Errichtung eines „Einreise-/Ausreisesystems“ (EES = Entry-Exit System), mithilfe dessen die Ein- und Ausreisebewegungen von Personen an den Grenzen des Schengen-Raums aufgezeichnet und Personen ausfindig gemacht werden sollen, die ihre per Visum genehmigte Aufenthaltsdauer in der EU überzogen haben (sogenannte „Overstayer“); (iii) die Einführung eines „Registrierungsprogramms für Reisende“ (RTP = Registered Traveller Programme), welches vorab überprüften Drittstaatenangehörigen (DSA), die nach bisherigen Erkenntnissen kein Sicherheitsrisiko für die EU darstellen, eine beschleunigte Einreise in den Schengen-Raum ermöglicht. Ob dies eine angemessene Reaktion auf die vergleichsweise geringe Zahl an Flüchtlingen ist, die während der jüngsten politischen Umbrüche aus Nordafrika nach Europa kamen, ist ein Argument, das vorzubringen sich praktisch gar nicht lohnt.[4] Die Vorschläge wurden bereits vor einiger Zeit erarbeitet und werden seit über vier Jahren aktiv diskutiert, auch wenn die EU-Institutionen erst vor kurzem mit der Ausarbeitung formeller Rechtsvorschriften begonnen haben.

Man hat uns gebeten, die drei genannten Vorschläge auf ihre Übereinstimmung mit der Charta der Grundrechte der Europäischen Union zu untersuchen und sie vor dem Hintergrund ihrer zu erwartenden Kosten, Folgen und Wirksamkeit zu bewerten. Bevor diese Fragen untersucht werden, muss darauf verwiesen werden, dass die gesetzliche Grundlage für EUROSUR im Dezember 2011 geschaffen wurde, wohingegen die rechtliche Verankerung des EES und RTP, die für den Frühsommer 2012 erwartet war, nun auf Ende des Jahres verschoben wurde. Wir mussten daher auf frühere Durchführbarkeitsstudien zurückgreifen und uns mit den relevanten Ausführungen zu diesem Thema in den EU-Institutionen behelfen. Eine weitere Herausforderung für diese Studie war die Tatsache, dass die Entwicklung von EUROSUR im Zuge eines im Februar 2008 von der Europäischen Kommission herausgegebenen „Fahrplans“ bereits in vollem Gange ist. Daher ging es nicht nur darum, die gesetzliche Grundlage zu analysieren, sondern es war gleichsam wichtig, auch die Umsetzung des Systems zu untersuchen.

---

1 Dokument des Rates 18666/11 ADD 1, S. 7.

2 „EU unveils plans for biometric border controls“ („EU gibt Pläne für biometrische Grenzkontrollen bekannt“), EUobserver, 13. Feb. 2008, abrufbar unter: http://euobserver.com/22/25650.

3 Siehe Schlussfolgerungen des Rates vom 11. und 12. Apr. 2011, sowie 9. und 10. Juni 2011.

4 Schätzungen des UNHCR zufolge flohen im Juni 2011 rund 1 Million Menschen aus Libyen in umliegende Länder wie Tunesien, Ägypten, Algerien, Niger und Tschad. UNHCR, Update Nr. 29, “Humanitarian situation in Libya and the neighbouring countries“ („Humanitäre Situation in Libyen und den Nachbarländern“), UNHCR 15. Juni 2011, abrufbar unter: http://www.unhcr.org/4df9cde49.html.

Kapitel 2 dieses Berichts untersucht die Ausarbeitung des vorgeschlagenen EUROSUR-Systems, des Einreise-/Ausreisesystems und des Registrierungsprogramms für Reisende. In Kapitel 3 wird beleuchtet, inwiefern die drei geplanten Systeme mit den wichtigsten Aspekten der EU-Grundrechtecharta übereinstimmen. Kapitel 4 konzentriert sich darauf, wie viel die EU bereits in EUROSUR und „Smart Borders“ investiert hat, und auf die geschätzten Kosten für die Umsetzung der Vorschläge. Der Bericht endet mit Schlussfolgerungen und Empfehlungen in den Kapiteln 5 und 6.

2 „Intelligente Grenzen“ für die Europäische Union?

Das Konzept „intelligenter Grenzen“ gewann in der EU an Glaubwürdigkeit, als die Europäische Kommission im Februar 2008 die sogenannte „Initiative für intelligente Grenzen“ ins Leben rief. Die Vorschläge umfassten automatische Identitätskontrollen, Kontrollgates, verstärkte Maßnahmen zur Vorkontrolle sowie neue Datenbanken, und gingen mit einem Fahrplan für die Ausarbeitung des Europäischen Grenzkontrollsystems einher. Im Rahmen von „EUROSUR“ sollen Küstenradar, Satellitensuchsysteme, Drohnen und automatische Erkennungssysteme eingesetzt werden, um kleine Boote mit Kurs auf EU-Hoheitsgebiet auszumachen.

„In diesem Paket steckt eine komplett neue Art der Grenzkontrolle“, so der frühere EU-Kommissar Franco Frattini über die Vorschläge von 2008. Die zugrundeliegende Annahme ist, dass die mit neuen Technologien ausgestatteten „intelligenten Grenzen" sowohl die Sicherheit erhöhen – indem Bedrohungen und Risiken (automatisch) erkannt werden – als auch für verbesserte Effizienz sorgen, z. B. durch stärkere Automatisierung und verkürzte Wartezeiten für Reisende bei der Passkontrolle. „Es gibt keine Alternative“, verkündete EU-Kommissar Frattini damals. „Die Gründe sind terroristische Bedrohungen, Kriminalität, pädophile Netze. Wir können nicht zulassen, dass solche Verbrecher bessere Technologien verwenden als die Polizei.“[5]

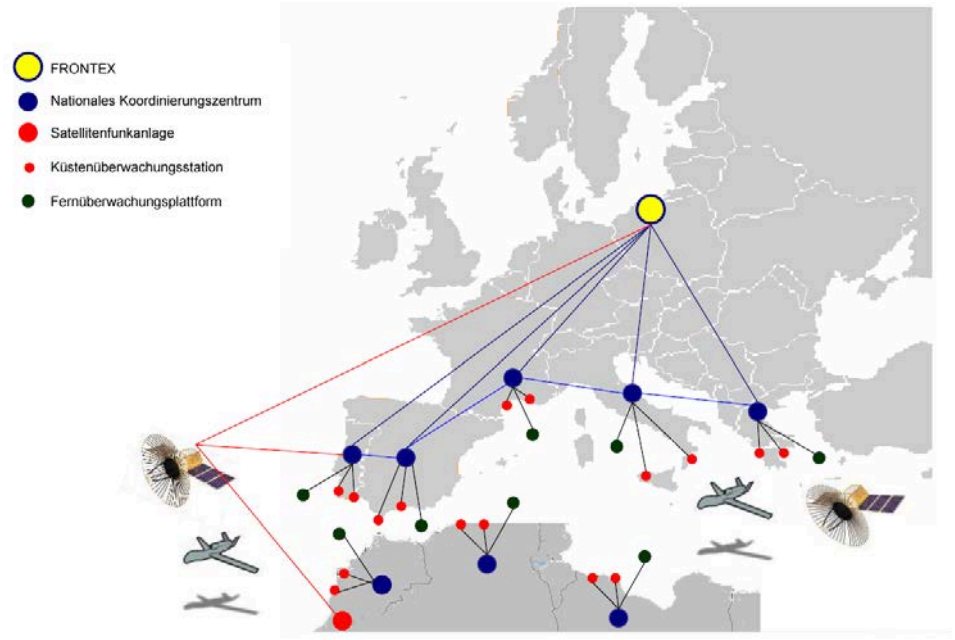
Wir sind grundsätzlich besorgt, dass zentrale Annahmen bezüglich der Notwendigkeit und der Wirksamkeit dieser Initiative nicht gründlich und unparteiisch überprüft worden sind. Zudem haben wir Bedenken, was den zugrunde liegenden blanken Ehrgeiz und den potenziellen Wirkungsbereich von EUROSUR und die Vorschläge zu „intelligenten Grenzen" angeht. Zusammen würden diese Maßnahmen in einer verstärkten Überwachung der EU-Grenzgebiete und der angrenzenden offenen Gewässer resultieren und zur Erhebung personenbezogener Daten von Millionen von Personen führen. Darüber hinaus hegen wir ernsthafte Zweifel an der technischen Durchführbarkeit der Pläne und stellen infrage, inwiefern es tatsächlich möglich sein wird, die Informationssysteme zahlreicher EU-Agenturen mit einer großen Menge nationaler und internationaler Überwachungssysteme so abzustimmen, dass bis zu 30 verschiedene einzelstaatliche Einwanderungs- und Grenzkontrollsysteme den erforderlichen operativen Standards entsprechen.

Mit Blick auf die „Smart Borders“-Initiative und eine solch hochtechnologische Reaktion auf Migrationsbewegungen, wie EUROSUR es ist, stellt sich auch eine politische Frage. Die EU macht angesichts vermeintlicher Migrationsprobleme zunehmend von technischen Lösungen Gebrauch. Häufig werden diese technischen Lösungen dann schlicht als technische Maßnahmen präsentiert, die unabhängig von der allgemeinen Migrations- und Grenzschutzpolitik der EU existieren (und daher nicht im selben Maße überprüft oder diskutiert werden müssen), obwohl sie in Wirklichkeit ein immer zentralerer Bestandteil dieser Politik werden. Wir hoffen, dass dieser Bericht dazu beiträgt, ein besseres Verständnis der Bedeutung solcher Technologien – und ihrer Anbieter – für die EU-Strategien zur Migrationskontrolle zu schaffen und er eine dringend erforderliche, umfassende Debatte über die moralischen, ethischen und rechtlichen Verpflichtungen Europas gegenüber Migrant/-innen und Flüchtlingen in Gang bringt.

5 „EU unveils plans for biometric border controls“, EUobserver, 13. Feb. 2008, abrufbar unter: http://euobserver.com/22/25650.

2.1 EUROSUR: Das Europäische Grenzkontrollsystem

Abbildung 1: Das geplante EUROSUR-System[6]



Die Entwicklung des EUROSUR-Systems kann als Teil eines langfristigen politischen Prozesses angesehen werden. Der Vertrag von Amsterdam aus dem Jahr 1999 räumte der EU erweiterte Befugnisse für nationale Grenzkontrollen und einwanderungs- und asylpolitische Belange ein und wies der Europäischen Kommission eine neue Rolle bei der Ausarbeitung von EU-Rechtsvorschriften zu. Allerdings waren es die Mitgliedstaaten, die bezüglich neuer politischer Initiativen der EU ambitionierte Ziele wie eine EU-Grenzpolizei und einen „globalen Migrationsansatz" forderten[7] – ersteres basierend auf dem Bedürfnis, den Mittelmeerraum zu kontrollieren und die Ankunft irregulärer Migrant/-innen und Flüchtlinge zu verhindern, und letzteres bezüglich der Externalisierung und Einführung von EU-Kontrollen in den Herkunfts- und Transitstaaten. Das nun geplante EUROSUR-System ist gewissermaßen das Ergebnis dieses dualen Ansatzes. Die im Folgenden behandelten Vorschläge sollten zudem vor dem Hintergrund der Mitteilung der Europäischen Kommission über „integrierten Grenzschutz" von 2002 betrachtet werden, im Zuge derer ein gemeinsamer „Schengener Grenzkodex", ein Leitfaden für Grenzposten sowie die Schaffung eines „Außengrenzenfonds" zur Stärkung von Kontrollen in den Mitgliedstaaten beschlossen wurden.[8]

6 GLOBE Projekt-Präsentation, abrufbar unter: http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=5119.

7 Dokument des Rates 13147/01.

8 KOM (2002) 233 endgültig. Siehe auch das Haager Programm von 2004. Der Grenzkodex wurde 2006 angenommen (Verordnung 2006/562/EG) und dem Außengrenzenfonds wurden für den Zeitraum 2007–2013 1,82 Milliarden Euro zugewiesen.

Der EU-Gesamtansatz zur Migrationsfrage wurde zwar offiziell erst 2005 angenommen, geht aber auf das Jahr 1997 zurück, als tausende kurdische Flüchtlinge aus dem Irak sich von der Türkei aus per Schiff auf den Weg nach Italien und Griechenland machten. Daraufhin legte die EU einen 46-Punkte-Plan vor, der sicherstellen sollte, dass diese Art des „Massenzustroms" in Zukunft verhindert würde.[9] Auf den Aktionsplan zum „Flüchtlingsstrom aus dem Irak und den Nachbarregionen" folgte ein von der österreichischen Ratspräsidentschaft vorgelegtes Strategiepapier zur Migrationspolitik. In diesem hieß es ausdrücklich, dass ein:

> [M]odell für eine Migrationspolitik der konzentrischen Kreise das Konzept der „Festung Europa" ablösen könnte ... die Schengen-Staaten verfügen derzeit über die schärfsten Kontrollmaßnahmen. Deren Nachbarländer könnten allmählich in ein ähnliches System eingebunden werden ... insbesondere, was Visumkontrollen und die Rückübernahmepolitik angeht. Ein dritter Ring von Staaten (GUS-Raum, Türkei und Nordafrika) wiederum würde sich vornehmlich auf Transitkontrollen und die Bekämpfung von Schleusernetzen konzentrieren, ein vierter Ring (Naher Osten, China, Schwarzafrika) auf die Reduzierung von Push-Faktoren.[10]

Von Migrant/-innen- und Flüchtlingsorganisationen hagelte es Kritik für das österreichische Strategiepapier, und auch die EU lehnte es ab,[11] nur um die Grundsätze dann doch 2002 in einen EU-Aktionsplan zu illegaler Einwanderung aufzunehmen.[12] Dieser Plan sah EU-Fördermittel für Migrationskontrollen in den Herkunftsländern von Migrant/-innen und Flüchtlingen vor, so zum Beispiel Förderung der Sachkompetenz und Bereitstellen der Ausrüstung für Grenzkontrollen, Unterstützung der Infrastruktur im Asylbereich, Entwicklung öffentlicher Registerstrukturen (also Biometrik/Datenbanken), Schaffung von Aufnahmeeinrichtungen für illegale Einwanderinnen und Einwanderer in Transitländern sowie „Sensibilisierungsmaßnahmen" für etwaige zukünftige „illegale" Emigrant/-innen. Der Aktionsplan forderte zudem für Abkommen zwischen der EU und Drittstaaten die Einführung von Bestimmungen zum „Migrationsmanagement", wobei mit dem Konzept von „Hilfe und Handel" die Kooperation der Drittstaaten gesichert wurde. Die Europäische Kommission begann mit der Finanzierung von „vorbereitenden Maßnahmen für die Zusammenarbeit mit Drittländern im Bereich Migration"aus dem Entwicklungshaushalt der EG (siehe Kapitel 4).[13]

Nach einem EU-Sondergipfel zum Thema Migration wurde im Dezember 2005 der „globale Ansatz" offiziell ausgeweitet, um erstmalig ein „Überwachungssystem, das alle südlichen Seegrenzen der EU und das Mittelmeer abdeckt", in Betracht zu ziehen.[14] Die nun offiziell eingerichtete Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union (FRONTEX)[15] wurde gebeten, eine Machbarkeitsstudie auf den Weg zu bringen.

9 Dokument des Rates 5573/98.

10 Dokument des Rates 9809/98.

11 „EU Migration plan side-lined and resurrected" („EU-Migrationsplan erst beiseitegeschoben und dann wieder aufgegriffen"), Statewatch Bulletin 8(6) (Nov.–Dez. 1998).

12 Dokument des Rates 6621/1/02.

13 Dieses Programm entwickelte sich schließlich zu der AENEAS-Haushaltslinie – einem für die Laufzeit 2004-2008 mit 250 Millionen Euro finanzierten Programm zur Verbesserung von Migrationskontrollen in Herkunfts- und Transitländern von Migrant/-innen und Flüchtlingen. Das Programm wurde mittlerweile in thematisches Programm für die Zusammenarbeit mit Drittländern in den Bereichen Migration und Asyl umbenannt und verfügt über ein Jahresbudget von etwa 75 Millionen Euro.

14 Schlussfolgerungen des Vorsitzes, Europäischer Rat, 15./16. Dez. 2005 [eigene Hervorhebung]. Siehe auch KOM (2005) 621 endgültig.

15 Verordnung (EG) Nr. 2007/2004.

Zudem wurde FRONTEX mit einer zweiten Durchführbarkeitsstudie über ein „Küstenpatrouillennetz für das Mittelmeer unter Beteiligung von EU-Mitgliedstaaten und nordafrikanischen Ländern“ beauftragt. FRONTEX führte beide Studien mithilfe von Sachverständigen verschiedener Mitgliedstaaten und der Gemeinsamen Forschungsstelle der EU durch. Die „MEDSEA“-Machbarkeitsstudie über ein Küstenpatrouillennetz für das Mittelmeer wurde den Mitgliedstaaten im Juli 2006 vorgelegt und später veröffentlicht.[16] Die „BORTEC“-Studie über das EU-Grenzkontrollsystem wurde den Mitgliedstaaten im Januar 2007 präsentiert, wurde jedoch als vertraulich eingestuft und ist bis dato nicht veröffentlicht worden. Die Empfehlung der MEDSEA-Studie war die Schaffung einer ständigen Organisationsstruktur zur „Kontrolle und Überwachung“ der gesamten südlichen Seeaußengrenzen der EU. Alle beteiligten Mitgliedstaaten sollten ein nationales Koordinierungszentrum (NKZ) einrichten, um mit FRONTEX, den anderen Mitgliedstaaten und ggf. Drittstaaten zusammenarbeiten zu können. Im Dezember 2006 ersuchte der Europäische Rat die Grenzschutzagentur FRONTEX, so rasch wie möglich ein ständiges Europäisches Küstenpatrouillennetz (EKPN) einzurichten, „um die illegale Einwanderung an den südlichen Seegrenzen einzudämmen“.[17] Die gemeinsamen Patrouillen von Grenzposten, Küstenwachen und Seestreitkräften konzentrierten sich ursprünglich auf die Kanarischen Inseln und das Gebiet südlich der Iberischen Halbinsel (geleitet von Portugal und Spanien) sowie auf den nördlichen Mittelmeerraum (Frankreich) und die nördliche Adria (Italien und Slowenien). Mittlerweile beteiligen sich zehn Mittelmeerländer am EKPN, eine externe Überprüfung seiner Wirksamkeit steht jedoch noch aus.[18]

In der BORTEC-Studie wurden die Möglichkeiten zur Küstenüberwachung von sieben Mitgliedstaaten untersucht[19] und die Einrichtung des Systems empfohlen, das später als EUROSUR bekannt werden sollte. Grundlage sollte eine verstärkte Küstenüberwachung durch die nationalen Koordinierungszentren des EKPN sowie der Datenaustausch untereinander und mit FRONTEX sein. Weiterhin wurde die Empfehlung ausgesprochen, „ernsthaft zu erwägen, Sensoren sowie unbemannte Luft- und Raumfahrzeuge“ einzusetzen, um Schiffe „jeder Größe und Beschaffenheit“ ausmachen und ihre Geschwindigkeit und ihren Kurs „bei jedem Wetter/Seegang, Tag und Nacht“ bestimmen zu können.[20] Überwacht würden alle Küstengewässer der EU in einem Radius von 30 Seemeilen sowie „breite Meeresgebiete nahe den Küstengewässern von Drittstaaten ... Entlang des südlichen Mittelmeerraums, von der Straße von Gibraltar bis nach Zypern, einschließlich des Ägäischen Meeres und Teilen der Adria [sowie] entlang der Westküste Afrikas.“[21]

Neben dem Küstenpatrouillennetz und EUROSUR unter der Leitung von FRONTEX stellte die Europäische Kommission im Oktober 2007 eine „integrierte Meerespolitik für die Europäische Union“ vor. Diese Strategie impliziert, dass EUROSUR letztendlich Teil eines „interoperable[n] Überwachungssystem[s] [sein wird, welches eingeleitet wird], um bestehende Schiffsüberwachungs- und -verfolgungssysteme, die für die Sicherheit auf See eingesetzt werden, sowie Systeme zum

16 Dokument des Rates 12049/06 EXT 1.

17 Schlussfolgerungen des Vorsitzes, Europäischer Rat, 14./15. Dez. 2006. Siehe auch die EU-Pressemitteilung zum EKPN, MEMO/07/203, 24. Mai 2007.

18 Bei den Ländern handelt es sich um Bulgarien, Zypern, Spanien, Frankreich, Griechenland, Italien, Malta, Portugal, Rumänien und Slowenien.

19 Zypern, Frankreich, Griechenland, Italien, Malta, Portugal, Slowenien und Spanien.

20 BORTEC-Studie, S. 105.

21 BORTEC-Studie, S. 98–99.

Schutz der Meeresumwelt, zur Fischereikontrolle, zur Kontrolle der Außengrenzen sowie für weitere Rechtsvollzugstätigkeiten auf See zusammenzubringen."[22] Auch soll unter der Leitung der Europäischen Verteidigungsagentur ein Meeresüberwachungsnetz für die Verteidigungsgemeinschaft entwickelt werden.[23] Beide Initiativen könnten bedeutende Folgen für die Ausarbeitung und praktische Anwendung des vorgeschlagenen EUROSUR-Systems haben.

Und schließlich ist es wichtig, die Rolle zu verstehen, die EUROSUR potenziell im Kontext rechtlicher und politischer Debatten über die Zulässigkeit gemeinsamer EU-Einsätze zur Migrationskontrolle unter der Leitung von FRONTEX oder im Kontext bilateraler Zusammenarbeit bzw. der Kooperation zwischen den Staaten einer Region untereinander spielen könnte. Hierbei sind zwei Punkte zu bedenken. Erstens sogenannte „Push-Back"-Operationen, in denen Personen beim Versuch der Einreise nach Europa in ihr jeweiliges Herkunftsland oder einen Drittstaat außerhalb der Europäischen Union zurückgeführt werden und somit keine Möglichkeit bekommen, in einem EU-Mitgliedstaat einen Asylantrag zu stellen. Der Europäische Gerichtshof für Menschenrechte entschied 2012 in einer Grundsatzentscheidung, Italien habe effektiv eine „Kollektivausweisung" vorgenommen, als die italienische Küstenwache 2009 auf hoher See ein Boot mit Flüchtlingen aufgriff und nach Libyen zurückbrachte. Die Flüchtlinge seien dadurch einem inakzeptabel hohen Risiko der Folter und Misshandlung ausgesetzt worden und Italien habe gegen seine Verpflichtung zur Nicht-Zurückweisung (*non-refoulement*) verstoßen.[24] In einem anderen Fall, den das Europäische Parlament vor den Europäischen Gerichtshof (EuGH) brachte, empfahl der Generalanwalt kürzlich eine Aufhebung der Richtlinien für gemeinsame Frontex-Einsätze.[25] Der Fall basiert auf einer gerichtlichen Anfechtung infolge des Entschlusses der Europäischen Kommission, das Europäische Parlament und den Europäischen Rat vom Rechtsetzungsprozess auszuschließen. Der Generalanwalt des EuGH erkannte jedoch an, dass das Verfahren offenbar genau deshalb eingeleitet worden war, weil es unter den Mitgliedstaaten Meinungsverschiedenheiten über die Geltung des Grundsatzes der Nicht-Zurückweisung bei extraterritorialen Einsätzen und die Bestimmung des Ortes, an den abgefangenene bzw. gerettete Personen zu verbringen sind, gibt.[26] Die von der Kommission zusätzlich zum Schengener Grenzkodex verabschiedeten Regelungen besagen, dass bei gemeinsamen Einsätzen

> „die Ausschiffung vorrangig in dem Drittland erfolgen [sollte], von dem aus das Schiff mit den Personen in See gestochen ist oder durch dessen Hoheitsgewässer oder Such- und Rettungszone dieses Schiff gereist ist; falls dies nicht möglich ist, sollte die Ausschiffung vorrangig im Aufnahmemitgliedstaat erfolgen, sofern nicht eine andere Vorgehensweise erforderlich ist, um die Sicherheit dieser Personen zu gewährleisten".[27]

22 KOM(2007) 575 endgültig.

23 Siehe „Maritime surveillance" („Meeresüberwachung"), Europäische Verteidigungsagentur, abrufbar unter: http://www.eda.europa.eu/otheractivities/maritimesurveillance.

24 Hirsi Jamaa und andere gegen Italien, Nr. 27765/09.

25 Beschluss 2010/252/EU des Rates vom 26. April 2010 zur Ergänzung des Schengener Grenzkodex hinsichtlich der Überwachung der Seeaußengrenzen im Rahmen der von der Europäischen Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union koordinierten operativen Zusammenarbeit.

26 Schlussanträge des Generalanwalts Paolo Mengozzi, 17. April 2012, Rechtssache C-355/10, Europäisches Parlament gegen Rat der Europäischen Union, Absatz 64.

27 Beschluss 2010/252/EU des Rates, Artikel 2, Teil II.

Die Zweideutigkeit der Bestimmungen zeigt sich z. B. daran, dass Malta sich nicht an FRONTEX-Einsätzen beteiligt aus Angst, gemäß den Richtlinien Personen in Seenot aufnehmen zu müssen. Gleichsam kritisieren Menschenrechtsverteidiger/-innen, dass die Regelungen zu mehr Zurückweisungen (*refoulement*) führen. Ein zweiter, verwandter Punkt ist die gemäß internationalem Recht übergeordnete Verpflichtung europäischer Schiffskapitäne zur Rettung irregulärer Migrant/-innen in Seenot sowie die ähnlich unklaren Verfahren zur Einleitung und Vornahme von Such- und Rettungseinsätzen.

Diese Debatten sind mit Bezug auf EUROSUR deshalb wichtig, weil die neuen Überwachungstechnologien potenziell für beide Zwecke eingesetzt werden könnten: zum Verhindern der Ankunft von Migrant/-innen und Flüchtlingen oder für Such- und Rettungseinsätze zur Minderung der haarsträubenden Zahl der Menschen, die im Mittelmeerraum wegen schlecht ausgerüsteter oder überladener Boote umkommen. Die Legitimität des EUROSUR-Systems wird vor allem daran gemessen werden, welchem dieser beiden Ziele Priorität eingeräumt wird. Gleichzeitig bewegen sich die Themen Abfangen, Zurückdrängen und Durchführen von Such- und Rettungseinsätzen eindeutig in einem Spannungsfeld. Die mangelnde Bereitschaft vonseiten der EU-Mitgliedstaaten, Verantwortung für Flüchtlinge und Asylbewerber/-innen zu übernehmen, trägt zum einen zu einer Präferenz von „Push-Back"-Operationen bei und führt zum anderen zu einer offensichtlichen Widerwilligkeit, verstärkt Such- und Rettungseinsätze durchzuführen, da wiederum keine Einigkeit darüber besteht, was mit den „Geretteten" geschehen soll.

Diese politische Uneinsichtigkeit hat tödliche Folgen. Im März 2012 veröffentlichte der Europarat einen vernichtenden Bericht über den Tod von 63 Personen, die auf einem Boot im Mittelmeer verhungert sind, nachdem sie tagelang vergeblich Notsignale ausgesendet hatten – obwohl Schiffe und Flugzeuge der NATO sich ganz in der Nähe aufhielten und die italienische Küstenwache Alarm schlug.[28] Der Bericht des Europarats konstatierte ein „kollektives Versagen" vonseiten der NATO und der europäischen Küstenwachen, und rief zu weiteren Untersuchungen auf. Im April leiteten Menschenrechtsgruppierungen rechtliche Schritte gegen das französische Verteidigungsministerium ein, und es werden im Anschluss daran noch weitere Verfahren erwartet.

2.1.1 Der EUROSUR-Fahrplan

Im Februar 2008 gab die Europäische Kommission eine Mitteilung zu EUROSUR heraus, in der sie die Ausarbeitung des EUROSUR-Systems ankündigte. Die gleichzeitig ausgesprochene Aufforderung an das Europäische Parlament, „die in dieser Mitteilung vorgebrachten Empfehlungen zu erörtern", hatte somit den Beigeschmack einer bloßen Pflichtübung.[29] EUROSUR sollte in drei Phasen und acht Schritten umgesetzt werden (siehe Kasten 1). Die Kommission kündigte überdies an, eine technische Studie in Auftrag geben zu wollen, um die Systemarchitektur zu entwerfen und eine Kostenschätzung zu erstellen. In der Folge wurden das Europäische Parlament und die nationalen Parlamente faktisch vor vollendete Tatsachen gestellt, was die Frage angeht, welche Art Grenzüberwachungssysteme europaweit eingeführt werden sollen (falls überhaupt).

28 „Lives lost in the Mediterranean Sea: who is responsible?" („Verlorene Leben im Mittelmeer: wer ist verantwortlich?"), Parlamentarische Versammlung des Europarates, 29. März 2012, abrufbar unter: http://assembly.coe.int/CommitteeDocs/2012/20120329_mig_RPT.EN.pdf.

29 KOM(2008) 68 endgültig.

Kasten1: Der EUROSUR-Fahrplan[30]

PHASE 1: Modernisierung und Ausweitung nationaler Grenzüberwachungssysteme und Einbindung nationaler Infrastrukturen in ein Kommunikationsnetz

- **Schritt 1:** Einrichtung von nationalen Koordinierungszentren in denen Mitgliedstaaten, die „in der Lage [sind], ein Situationsbewusstsein über die Bedingungen und Aktivitäten entlang der Außengrenzen aufzubauen sowie alle notwendigen Instrumente bereitzustellen, um entsprechend zu reagieren."
- **Schritt 2:** Errichtung eines gesicherten computergestützten Kommunikationsnetzes, damit „Daten rund um die Uhr in Echtzeit sowohl zwischen nationalen Zentren als auch mit FRONTEX ausgetauscht werden können."
- **Schritt 3:** Verstärkung der finanziellen und logistischen Hilfe seitens der EU für die Unterstützung benachbarter Drittländer bei der Errichtung einer Grenzüberwachungsinfrastruktur.

PHASE 2: Entwicklung und Einführung gemeinsamer Instrumente und Anwendungen zur Grenzüberwachung auf EU-Ebene

- **Schritt 4:** Forschung und Entwicklung zur Steigerung der Leistungsfähigkeit von Überwachungsinstrumenten, insbesondere Erdüberwachungssatelliten und UAVs (Drohnen).
- **Schritt 5:** Entwicklung gemeinsamer Überwachungsinstrumente mit FRONTEX als Mittler.
- **Schritt 6:** Entwicklung von Überwachungssystemen für die offene See, welche ein „gemeinsames Informationsbild des Grenzvorbereichs" liefern.

PHASE 3: Schaffung eines gemeinsamen Überwachungs- und Informationsraums für den maritimen Bereich der EU, in dem alle relevanten Daten aus nationalen Überwachungssystemen, neuen Überwachungsinstrumenten, europäischen und internationalen Meldesystemen und nachrichtendienstlichen Quellen systematisch erfasst, analysiert und zwischen den zuständigen nationalen Behörden verbreitet werden können.

- **Schritt 7:** Schaffung eines integrierten Netzes der Melde- und Überwachungssysteme zum Zwecke der Grenzkontrolle und inneren Sicherheit für das Mittelmeer, den südlichen Atlantik (Kanarische Inseln) und das Schwarze Meer. Durch die Kombination nachrichtendienstlicher Erkenntnisse mit Informationen, die aus Überwachungsinstrumenten gewonnen werden, könnten gemeinsame Informationsbilder des Grenzvorbereichs entwickelt werden.
- **Schritt 8:** Einrichtung eines integrierten Netzes aller europäischen Melde- und Überwachungssysteme für den maritimen Bereich, mit dem sämtliche maritimen Tätigkeiten wie Seeverkehrssicherheit, Schutz der Meeresumwelt, Fischereikontrolle und Rechtsdurchsetzung erfasst werden.

2.1.2 Der EUROSUR-Verordnungsvorschlag

Der EUROSUR-Verordnungsvorschlag wurde im Dezember 2011 von der Europäischen Kommission öffentlich gemacht.[31] Man hätte hier sicherlich darauf achten können, ihn zeitnaher nach Inkrafttreten des Vertrags von Lissabon vorzulegen, um eine ordentliche Diskussion über das Thema

30 Ebd.
31 KOM (2011) 873 endgültig, 12. Dez. 2011.

zu ermöglichen, bevor die weitreichenden Schritte zur Umsetzung des EUROSUR-Fahrplans unternommen wurden (mehr dazu in Kapitel 4).

Laut der Folgenabschätzung und Artikel 1 des Vorschlags erfüllt EUROSUR den Zweck, „das Lagebewusstsein und die Reaktionsfähigkeit der Mitgliedstaaten und der Agentur bei der Prävention von irregulärer Migration und grenzüberschreitender Kriminalität an den Land- und Seeaußengrenzen zu verbessern". In der Präambel des Vorschlags heißt es, dass EUROSUR zudem dem „Schutz und ... der Rettung von Migranten" dient.[32] Dies wird jedoch nicht ausdrücklich in Rechtsvorschriften festgehalten, sondern findet nur in Form eines allgemeinen Verweises auf die Wahrung der Grundrechte und die vorrangige Behandlung von gefährdeten Personen in besonders schwierigen Situationen, wie z. B. Personen in Seenot, Einzug in den Verordnungsvorschlag.[33] Die Bestimmungen zur Überwachung hingegen sind ausführlich, umfassend und so weit wie möglich gefasst.[34]

In der Praxis würde durch die Verordnung nicht nur ein umfassendes Europäisches Grenzkontrollsystem basierend auf einem komplexen „System-der-Systeme"-Ansatz konzipiert,[35] sondern auch die Verpflichtungen der Schengen-Staaten – derzeit die Vornahme von Grenzkontrollen und Überwachungsmaßnahmen zur Aufspürung krimineller Aktivitäten und Verhinderung illegaler Einwanderung – um eine sehr viel stärkere Auflage erweitert: Sie müssten alle diejenigen Land- und Seegrenzen umfassend und ununterbrochen überwachen, die von FRONTEX in puncto illegaler Einwanderung als Hochrisikogrenzen eingestuft werden. Überdies würde der aktuelle Status und Kompetenzbereich von FRONTEX durch den Verordnungsvorschlag erheblich

32 Erwägungsgrund 1.

33 Artikel 2(3).

34 Laut Artikel 3bezeichnet der Ausdruck a) „Lagebewusstsein" die Fähigkeit, grenzüberschreitende Aktivitäten zu beobachten, aufzuspüren, zu identifizieren, zu verfolgen und zu verstehen, um Kontrollmaßnahmen angemessen zu begründen, indem neue Informationen mit bereits bekannten Fakten kombiniert werden; b) „Reaktionsfähigkeit" die Fähigkeit, Maßnahmen durchzuführen, mit denen gegen illegale Grenzüberschreitungen vorgegangen werden soll, einschließlich der Mittel und des Zeitrahmens für eine angemessene Reaktion auf ungewöhnliche Umstände; c) „Lagebild" eine Schnittstelle zur grafischen Darstellung von Echtzeit-Daten, Informationen und nachrichtendienstlichen Erkenntnissen, die von verschiedenen Behörden, Sensoren, Plattformen und anderen Quellen erhalten wurden und mit anderen Behörden über Kommunikations- und Informationskanäle ausgetauscht werden, um ein Lagebewusstsein zu erlangen und die Reaktionsfähigkeit entlang den Außengrenzen und im Grenzvorbereich zu unterstützen; d) „grenzüberschreitende Kriminalität" jede Form von schwerer oder organisierter Kriminalität an den Außengrenzen der Mitgliedstaaten, wie Menschenhandel, Drogenschmuggel und sonstige rechtswidrige Handlungen; e) „Außengrenzabschnitt" die Gesamtheit oder einen Teil der Land- oder Seeaußengrenze eines Mitgliedstaats gemäß den innerstaatlichen Rechtsvorschriften oder entsprechend den Vorgaben des nationalen Koordinierungszentrums oder einer anderen zuständigen nationalen Behörde; f) „Grenzvorbereich" das geografische Gebiet jenseits der Außengrenze von Mitgliedstaaten, das nicht durch ein nationales Grenzüberwachungssystem erfasst ist [eigene Hervorhebung].

35 Einen detaillierten Überblick finden Sie in Kasten 2 auf S. 25. Die Europäische Verteidigungsagentur definiert ein „System der Systeme" als eine Reihe bzw. Anordnung von Systemen, die sich aufgrund räumlicher Distanzen oder unterschiedlicher Zuständigkeiten nicht für eine Überführung in ein einziges System eignen. „Bei Gemeinsamkeiten hinsichtlich Verfahren, verwendeter Datenbanken oder übergeordneter Ziele bietet sich eine gewisse Bündelung von Ressourcen zum Erzielen von Synergieeffekten, jedoch ohne Verlust der räumlichen und organisatorischen Unabhängigkeit, an. Eine solche Bündelung von Ressourcen kann zentral oder durch einen Zusammenschluss interessierter Fachleute erfolgen." Wise Pen Team, „Maritime surveillance in support of CSDP: The Wise Pen Team Final Report to EDA Steering Board", Apr. 2010, S. 48.

erweitert – von eben solchen Risikobewertungen über die Koordinierung gemeinsamer Einsätze bis hin zur Überwachung der Seegebiete auch über EU-Hoheitsgebiet hinaus (durch ein „gemeinsames Informationsbild des Grenzvorbereichs“ basierend auf einem Austausch von Informationen und nachrichtendienstlichen Erkenntnissen). Unter der Verordnung müssten zudem *alle* teilnehmenden Staaten – und nicht nur diejenigen mit Hochrisikogrenzen – beträchtliche Summen in die Anpassung ihrer eigenen Grenzkontrollsysteme an die Standards und Erfordernisse von EUROSUR investieren.

Das EUROSUR-System sieht vor, die Mitgliedstaaten über nationale Koordinierungszentren mit FRONTEX zu vernetzen.[36] Die NKZ müssen ein nationales Lagebild ihrer Küstenlinien und Hoheitsgewässer erstellen und regelmäßig aktualisieren „mit dem Ziel, allen Behörden mit Zuständigkeit für die Grenzüberwachung auf nationaler Ebene zweckmäßige, sachlich richtige und aktuelle Informationen an die Hand zu geben, die für die Prävention von irregulärer Migration und grenzüberschreitender Kriminalität ... von Belang sind“.[37] Weiter führt der Verordnungsvorschlag detailliert aus, dass das nationale Lagebild aus drei bestimmten „Schichten“ bestehen soll: einer Ereignissschicht, einer Einsatzschicht und einer Analyseschicht. Jede Schicht ist in drei oder vier „Teilschichten“ unterteilt. Zu einem späteren Zeitpunkt sollen auch die EU-Binnenstaaten in das EUROSUR-System eingebunden werden. Die NKZ wären verantwortlich für die Koordinierung nationaler Gegenmaßnahmen bei von FRONTEX/EUROSUR ausgemachten Sicherheitsbedrohungen, was faktisch eine Erweiterung des Mandats darstellt, über welches das bestehende Netzwerk an NKZ verfügt. Dieses Netz wurde von den Mitgliedstaaten eingerichtet, die Teil des 2006 gegründeten Europäischen Küstenpatrouillennetzes sind.[38] Von FRONTEX erarbeitete „freiwillige“ Richtlinien für die NKZ wurden 2009 angenommen[39] und später in den Schengen-Katalog über Außengrenzkontrollen aufgenommen.[40] Demnach sind die Schengen-Staaten verpflichtet, eine nationale Grenzschutzstrategie zu beschließen, ein NKZ einzurichten und die Überwachungsinfrastruktur zu entwickeln, die zur Beteiligung an EUROSUR nötig ist. Ende 2011 hatten 16 der 18 Mitgliedstaaten an den südlichen und östlichen Außengrenzen des Schengen-Raums ihre NKZ eingerichtet, und die meisten davon hatten 2011 die Arbeit aufgenommen.[41]

Das Pendant zu den NKZ ist das 2008 eingerichtete FRONTEX Situation Centre (FSC).[42] Der Informationsaustausch zwischen dem FSC und den NKZ erfolgt über ein gesichertes computergestütztes Kommunikationsnetz. So ist FRONTEX in der Lage, die „nationalen Lagebilder“ zu einem mehrschichtigen europäischen Lagebild zusammenzuführen, welches u. a. aus

36 Gemäß den Schengen-Sonderregelungen für das Vereinigte Königreich, Irland und Dänemark werden diese Länder EUROSUR nicht beitreten. Norwegen, Island, die Schweiz und Liechtenstein, die keine EU-Mitgliedstaaten sind, aber dem Schengen-Raum angehören, werden sich beteiligen.

37 Artikel 9. Das nationale Lagebild „wird ... zusammengestellt“ aus Informationen aus zahlreichen Überwachungssystemen: nationalen Grenzüberwachungssystemen; ortsfesten und mobilen Sensoren, die von den nationalen Behörden betrieben werden (Radar usw.); Grenzpatrouillen und sonstigen Beobachtungsmissionen; lokalen, regionalen und sonstigen Koordinierungszentren; sonstigen relevanten nationalen Behörden und Systemen; der Agentur; nationalen Koordinierungszentren anderer Mitgliedstaaten und von Drittländern; regionalen Netzwerken mit benachbarten Drittländern; Schiffsmeldesystemen wie dem automatischen Identifikationssystem AIS und dem Schiffsortungssystem VMS; und sonstigen Quellen.

38 Artikel 5.

39 FRONTEX-Entscheidung vom 10. März 2009, überarbeitet 23 Nov. 2010.

40 Dokument des Rates 7864/09.

41 SEK (2011) 1536 endgültig, 12. Dez. 2011, S. 15–16.

42 Siehe „FRONTEX one stop shop“, FRONTEX, abrufbar unter: https://foss.frontex.europa.eu/.

„Informationen ... zusammengestellt“ wird, die aus „*sonstige[n]* einschlägig befasste[n] europäische[n] und internationale[n] Organisationen [und aus] *sonstige[n]* Quellen“ stammen.[43] FRONTEX wird zudem für die Erstellung und Aktualisierung des gemeinsamen Informationsbildes des Grenzvorbereichs zuständig sein – faktisch bedeutet dies die Überwachung nicht-territorialer Gewässer und der Hoheitsgebiete von Drittstaaten. Das gemeinsame Informationsbild des Grenzvorbereichs soll aus Informationen bestehen, die von den NKZ, Verbindungsbeamten für Einwanderungsfragen in Drittstaaten, *sonstigen* einschlägig befassten europäischen und internationalen Organisationen, Drittländern und *sonstigen* Quellen bereitgestellt werden. Eine weitere Zuständigkeit von FRONTEX wird die „gemeinsame Anwendung von Überwachungsinstrumenten“ sein, so z. B. Satelliten, Schiffsmeldesysteme, Schiffsüberwachungssysteme und „auf Plattformen, einschließlich bemannten und unbemannten Fluggeräten, montierte Sensoren“.[44]

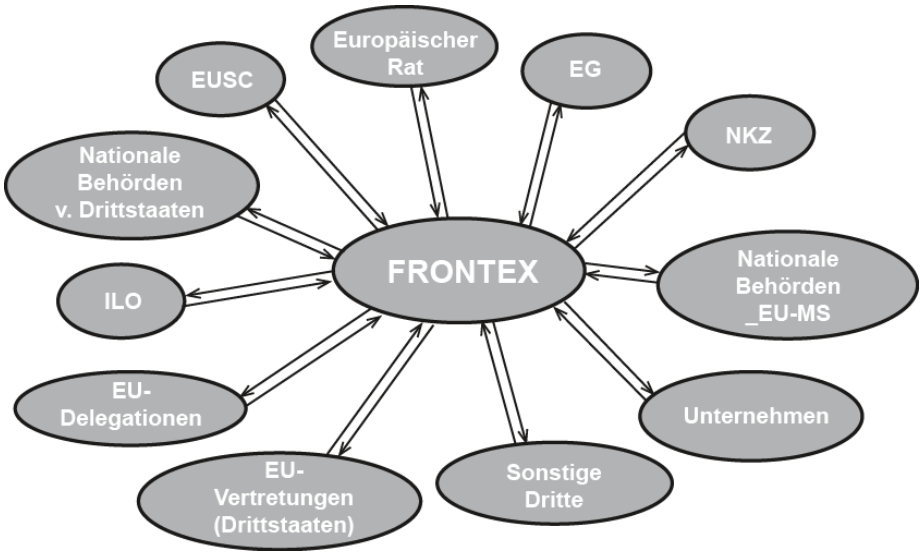
Zu guter Letzt wird in der Begründung des Verordnungsvorschlags betont, dass die „Zusammenarbeit mit benachbarten Drittländern ... für den Erfolg von EUROSUR von entscheidender Bedeutung [ist]“. Diese Zusammenarbeit soll auf früheren Anstrengungen aufbauen, die Herkunftsländer von Migrant/-innen und Flüchtlingen auf dem Weg nach Europa für eine Zusammenarbeit zu gewinnen (insbesondere die Länder Nord- und Westafrikas), indem man sie in das System zum Informationsaustausch einbindet. Die EU-Mitgliedstaaten haben ausgeklügelte Kooperationsmechanismen zum Informationsaustausch, der Rückführung „illegaler“ Migrant/-innen und der Kontrolle der nördlichen und westlichen Küstengewässer Afrikas zur Prävention „ unerlaubten Verlassens“ entwickelt. Letzteres ist eine ernste Entstellung der in der Allgemeinen Erklärung der Menschenrechte festgeschriebenen Garantie, dass *jeder* Mensch das Recht haben muss, *jedes* Land zu verlassen.[45] Solche Kooperationsabkommen, die mit der Bereitstellung von Ausrüstung und Sachkompetenz vonseiten der EU-Mitgliedstaaten einhergingen, bestanden vor allem mit Libyen (damals unter der Herrschaft von Muammar al-Gaddafi),[46] Tunesien (unter Ben Ali) und dem Königreich Marokko. Da sie jedoch auf bilateralen Verträgen basierten (bspw. zwischen Italien und Libyen oder zwischen Spanien und Marokko), entzogen sie sich jeder demokratischen und gerichtlichen Kontrolle auf europäischer Ebene. Die Umbrüche des Arabischen Frühlings haben diese Abkommen über den Haufen geworfen. Daher hat der Europäische Auswärtige Dienst vor kurzem eine „Bedarfsermittlungsmission für Grenzschutzangelegenheiten“ in Libyen eingerichtet.[47] Neben bilateralen Vereinbarungen gibt es zwischen EU-Mitgliedstaaten auch multilaterale, regionale Netzwerke zur Migrationskontrolle wie z. B. „SEAHORSE“ (weitere Informationen hierzu in Kapitel 4.3.2), die sich ebenfalls außerhalb des offiziellen Geltungsbereichs der EU-Bestimmungen bewegen.

Die EUROSUR-Bestimmungen sehen lediglich eine Beteiligung von Drittstaaten und regionalen Netzwerken am EUROSUR-Kommunikationsnetz vor; wie die so erhaltenen Informationen praktisch eingesetzt werden, wird kaum angesprochen. Derlei operative Entscheidungen werden der täglichen

43 Artikel 10, Verordnungsvorschlag [eigene Hervorhebung].
44 Artikel 12.
45 AEMR, Artikel 13.
46 „Dirty deals and unprincipled politics“ („Schmutzige Deals und gewissenlose Politik“), Transnational Institute, März 2011, abrufbar unter: http://www.tni.org/interview/dirty-deals-and-unprincipled-politics.
47 EAD, EU launches a needs assessment mission for border management in Libya („EU ruft Bedarfsermittlungsmission für Grenzschutzangelegenheiten ins Leben“), abrufbar unter: http://eeas.europa.eu/libya/docs/2012_lybia_border_management_en.pdf

Steuerung durch FRONTEX überlassen. Gemäß dem Verordnungsvorschlag können sich auch folgende Einrichtungen an EUROSUR beteiligen: EUROPOL, das Maritime Analysis and Operations Centre – Narcotics, das Centre de Coordination pour la lutte antidrogue en Méditerranée, die Europäische Fischereiaufsichtsagentur sowie weitere EU-Agenturen und internationale Organisationen.[48] Uns bereitet Sorge, dass eine potenziell unbegrenzte Zahl von Drittparteien – vor dem Hintergrund fehlender effektiver Beaufsichtigung des Informationsaustauschs zwischen diesen Parteien – bedeutet, dass das EUROSUR-System von Anfang an eine schleichende Ausweitung der Zweckbestimmung („function creep“) aufweist.

Abbildung 2**: Beteiligte Stellen am gemeinsamen Informationsbild des Grenzvorbereichs**[49]



2.1.3 Mehr als nur Grenzkontrollen: integrierte Meeresüberwachung

Im Oktober 2009 legte die Europäische Kommission zusätzlich zu der bereits veröffentlichten Mitteilung über eine „integrierte Meerespolitik“ eine weitere Mitteilung namens „Auf dem Weg zur Integration der Meeresüberwachung: Ein gemeinsamer Informationsraum [CISE] für den maritimen Bereich der EU“ vor.[50] Ein Jahr später folgte dann der „Entwurf eines Fahrplans für die Schaffung des gemeinsamen Informationsraums [CISE] für die Überwachung des maritimen Bereichs der EU“.[51] In diesen beiden Dokumenten wird vorgeschlagen, EUROSUR letztendlich in ein größeres System zu integrieren, das zahlreichen nationalen und internationalen Agenturen zur Verfügung steht, beispielsweise solchen verantwortlich für „Sicherheit auf See (einschließlich Such- und Rettungsdienste), Gefahrenabwehr in der Schifffahrt und Vermeidung von Umweltverschmutzung durch Schiffe; Fischereiaufsicht; Vorsorge- und Abhilfemaßnahmen im Bereich der

48 Artikel 17.

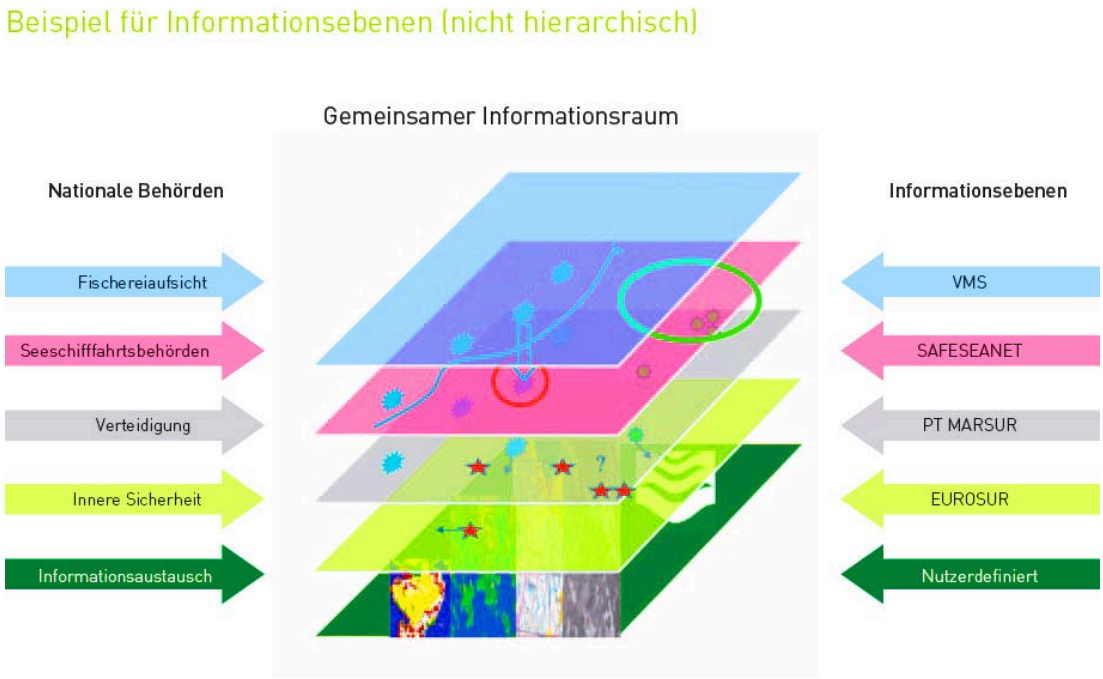
49 Quelle: ESG, “EUROSUR Technical Study – Subproject 3 Final Report – Common Pre-frontier Intelligence Picture” („EUROSUR: Technische Studie – Teilprojekt 3 endgültiger Bericht – gemeinsames Informationsbild des Grenzvorbereichs“), Jan. 2010, S. 59.

50 KOM (2009) 538 endgültig, 15. Okt. 2009.

51 KOM (2010) 584 endgültig.

Meeresverschmutzung; Meeresumwelt; Zoll; Grenzkontrolle; die allgemeine Durchsetzung von Rechtsvorschriften; Verteidigung."

Abbildung 3: EUROSUR und der Gemeinsame Informationsraum[52]



Eine umfassende Analyse aller möglichen Komponenten des Gemeinsamen Informationsraums ist zwar im Rahmen dieses Berichts nicht möglich, Kasten 2 geht jedoch kurz auf die wichtigsten „Informationsebenen" und Interessenvertreter ein, die aller Wahrscheinlichkeit nach an EUROSUR/CISE beteiligt sein werden.

Im Fahrplanentwurf für die Schaffung von CISE heißt es, dass „die gemeinsamen Bedürfnisse der meisten Nutzergruppen ... dazu bei[tragen], ... ein grundlegend verbessertes Bild der Lage im maritimen Bereich zu zeichnen. Dieses Bild kann sich aus Daten aus *einer Kombination von Systemen und Sensoren zusammensetzen, die kooperative und nicht-kooperative Zielobjekte jeder Größe erfassen können*".[53] Dies ist im Wesentlichen das Prinzip hinter EUROSUR, wie es auch in der BORTEC-Studie von FRONTEX beschrieben ist. Ebenfalls klar ist, dass die Europäische Kommission vorhat, es EUROSUR zu ermöglichen, in dieser Hinsicht mit einer großen Nutzergruppe zusammenzuarbeiten. Laut der Kommission wird das Europäische Grenzkontrollsystem „die Bedürfnisse und Instrumente aller Bereiche der Meeresüberwachung in einem gemeinsamen System zum Informationsaustausch zusammenführen, wie es in dieser [CISE-] Mitteilung dargelegt ist".[54] Was den Zweck des neuen Gemeinsamen Informationsraums angeht, so wird er laut des Fahrplanentwurfs zur Bereitstellung folgender Informationen genutzt werden:

52 KOM (2010) 584, S. 5.
53 Eigene Hervorhebung.
54 SEK (2009) 1341 endgültig, S. 3.

(a) Daten zu *illegalen Tätigkeiten und Bedrohungen unter Beteiligung von Schiffen*, die die innere und äußere Sicherheit der EU betreffen. Derartige Informationen werden vorrangig von Küstenwachen, Grenzschutz, Polizei und *Streitkräften* gesammelt.

(b) spezifische Fangdaten, kombiniert mit Positionsangaben von Fischereifahrzeugen zur *Bekämpfung des illegalen Fischfangs*.

(c) *erweiterte elektronische Daten zu allen Waren, die in EU-Zollgebiet verbracht oder aus ihm entfernt werden*, um eine erste Beurteilung der Sicherheit der Waren zu ermöglichen.[55]

Es scheint eindeutig, dass die Europäische Kommission plant, EUROSUR zum Zweck der Fischereikontrolle und zur Durchsetzung der Zollvorschriften einzusetzen und die nationalen militärischen Streitkräfte daran zu beteiligen. Dieser erweiterte Kompetenzbereich hätte im Verordnungsvorschlag dargelegt werden müssen, nicht zuletzt wegen der zu erwartenden Folgen für die Grundrechte. Stattdessen wird im Rahmen des Vorschlags lediglich der Weg dafür geebnet, unbegrenzt viele Datensätze und Agenturen in das System zu integrieren (siehe oben). Der Einsatz von EUROSUR für die oben genannten Zwecke mag ja u. U. gute Gründe haben – diese sollten jedoch von vornherein klar dargelegt werden. Andernfalls ist nur schwer vorstellbar, wie die Rechtsvorschriften, die die Grundlage für das EUROSUR-System bilden sollen, verabschiedet werden können, wenn stets die Möglichkeit besteht, dass der Wirkungsbereich und Einsatzzweck des Systems letztendlich viel weiter greifen könnten als das, was der Gesetzgeber bewilligen soll.

Kasten2: EUROSUR – Ein System der Systeme

Auflagen der Internationalen Seeschifffahrtsorganisation: AIS und LRIT

Laut Vorschriften der Internationalen Seeschifffahrtsorganisation müssen Fracht- und Passagierschiffe Daten übermitteln, die von Küstenbehörden mittels Radar oder Satellit empfangen werden können. Automatische Identifikationssysteme (AIS) übermitteln Informationen von mit Transpondern ausgerüsteten Schiffen. Zu diesen Daten zählen Angaben zur Identifikation des Schiffes sowie über Position, Geschwindigkeit, Kurs und allgemeine Informationen über seine Ladung.[56] Bei der Fernidentifizierung und -verfolgung (LRIT – Long Range Identification and Tracking) werden in regelmäßigen Abständen per Satellit Informationen zur Identität und Position eines Schiffes übermittelt, die dann von LRIT-Datenzentren empfangen werden. Die Bestimmungen der Internationalen Seeschifffahrtsorganisation sehen jedoch vor, dass nur der Flaggenstaat, der Staat des Bestimmungshafens (Hafenstaat) des Schiffes und Küstenstaaten im Radius von 1.000 Seemeilen Zugang zu den Daten haben sollen.[57] AIS und LRIT-Informationen sollen Teil des EUROSUR-Systems bilden.

EU-Fischereikontrolle und Schiffsüberwachungs- und -ortungssysteme (VMS/VDS)

Schiffsüberwachungssysteme (VMS – Vessel Monitoring Systems) wurden im Rahmen der Gemeinsamen Fischereipolitik der EU ins Leben gerufen. Jeder Mitgliedstaat ist gesetzlich

55 KOM (2010) 584, S. 4 [eigene Hervorhebung].

56 Seit dem 31. Dezember 2004 müssen alle Schiffe ab 300 Bruttoregistertonnen, die internationale Fahrten unternehmen, sowie alle Frachter ab 500 Bruttoregistertonnen und alle Passagierschiffe egal welcher Größe mit AIS ausgerüstet sein.

57 Seit dem 31. Dezember 2008 müssen alle Passagier- und Frachtschiffe ab 300 Bruttoregistertonnen, die internationale Fahrten unternehmen, sowie bewegliche Offshore-Bohreinheiten LRIT-Informationen übermitteln.

verpflichtet, ein satellitenbasiertes VMS zur Überwachung der Position und des Kurses von Fischereifahrzeugen einzuführen.[58] Mithilfe von VMS werden in regelmäßigen Abschnitten Daten über ein Schiff übermittelt, aus denen sich Informationen wie z. B. die Geschwindigkeit und der Kurs des Schiffes ablesen lassen. Die Behörden verwenden VMS-Daten zur Überwachung von Fanggebieten und um sicherzustellen, dass ein Schiff alle nötigen Genehmigungen und Quoten für den Fischfang in dem jeweiligen Gebiet vorweisen kann. 2009 wurde die Gesetzgebung zur Fischereikontrolle geändert: aus dem Schiffsüberwachungssystem wurde das Schiffsortungssystem (VDS – Vessel Detection System) und es sollte ermöglicht werden, die von VMS, VDS und AIS gelieferten Daten zur Fischereikontrolle an die Gemeinschaftsagenturen und an die „an Überwachungseinsätzen beteiligten zuständigen Behörden der Mitgliedstaaten zum Zwecke der Sicherheit auf See, der Durchführung von Grenzkontrollen, des Schutzes der Meeresumwelt und allgemein der Durchsetzung geltender Vorschriften weiterzugeben“.[59]

SAFESEANET

Bei SAFESEANET handelt es sich um ein von der Europäischen Agentur für die Sicherheit des Seeverkehrs (EMSA) geleitetes Überwachungs- und Informationssystem für den Schiffsverkehr. Die EU-Mitgliedstaaten sowie Norwegen und Island können so Informationen über Schiffe, Schiffsbewegungen und Gefahrgut zur Verfügung stellen und erhalten, um einer Verschmutzung der Meeresumwelt vorzubeugen, den Transport von Gefahrgütern zu überwachen und Verstöße gegen Sicherheits- und Gesundheitsschutzvorschriften aufzudecken.[60] Zu SAFESEANET gehört ein EU-Überwachungs- und Informationssystem für den Schiffsverkehr, welches AIS-Positionsmeldungen und auf Grundlage sonstiger EU-Richtlinien bereitgestellte Daten – z. B. bezüglich Kontrollen der Hafenauffangeinrichtungen für Schiffsabfälle – bündelt. Laut EMSA werden durch SAFESEANET täglich die Bewegungen von 12.000 Schiffen in EU-Gewässern nachverfolgt und monatlich 100 Millionen AIS-Positionsmeldungen aufgezeichnet. SAFESEANET wurde als zentrales Indexsystem eingerichtet, dessen Funktionsweise an eine Telefonzentrale erinnert: Nicht die Daten an sich werden gespeichert, sondern nur Angaben zu den jeweiligen Speicherorten der Daten.

2010 erweiterte die EMSA das SAFESEANET-Informationssystem um ein Modul zur Nachverfolgung von Schiffen. Das SAFESEANET-Modul für ein Verkehrsinformationsweiterleitungs- und -austauschsystem STIRES bündelt Informationen aus Hafenbenachrichtigungen, Schiffsbenachrichtigungen (basierend auf AIS-Daten), Gefahrgutbenachrichtigungen und Schadensberichten. Der Direktor der EMSA, Willem de Ruiter, meint: „Dieser Ansatz wird den Mitgliedstaaten eine ganze Reihe wichtiger neuer Ressourcen zur Verfügung stellen ... Statt einfach nur Zugang zu einer Datenbank zu haben, können sie auf einer Karte die gesamte europaweite Situation beinahe in Echtzeit überblicken und alle Schiffe, Häfen, Seegebiete und viele andere Elemente mit nur einem Klick auswählen. Und noch besser: Bald werden wir in der Lage sein, ein integriertes Display-System anzubieten, das Schiffe weltweit identifizieren und orten und zudem Grafiken zu Umweltverschmutzung und Unfällen in der EU erstellen kann. Die Zahl der Nutzer steigt stetig. Zuletzt sind die Beamten der Hafenstaatkontrolle dem System beigetreten.“[61] 2010 wurde

58 Richtlinie 2002/59/EG. Seit dem 1. Januar 2005 müssen alle Gemeinschaftsschiffe über 15 Meter Länge mit Satellitenüberwachungsanlagen für VMS ausgestattet sein. Ausgenommen sind Fischereifahrzeuge, die ausschließlich für Zwecke der Aquakultur eingesetzt werden und ausschließlich innerhalb der Basislinien der Mitgliedstaaten operieren. Ein in Gemeinschaftsgewässern tätiges Drittlandschiff, das den Bestimmungen für VMS unterliegt, muss eine funktionstätige Satellitenüberwachungsanlage an Bord installiert haben.

59 Artikel 11 und 12, Richtlinie 2009/17/EG.

60 Richtlinie 2002/59/EG (geändert durch die Richtlinie 2009/17/EG) über die Einrichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr. Siehe auch „SafeSeaNet“, Europäische Agentur für die Sicherheit des Seeverkehrs, abrufbar unter: http://www.emsa.europa.eu/operations/maritime-surveillance/safeseanet/113-safeseanet.html.

61 „EMSA Launches New, Map-based Shipping Surveillance System“ („EMSA führt neues, kartenbasiertes Schiffsüberwachungssystem ein“), EMSA-Pressemitteilung, 10. März 2010, abrufbar unter: http://www.emsa.europa.eu/news-a-press-centre/external-news/download/296/2/23.html.

im westlichen Mittelmeerraum ein Pilotprojekt zur Zusammenführung von Daten aus VMS und dem SAFESEANET-Informationssystem ins Leben gerufen. Geleitet wird das Projekt von EMSA, unter Beteiligung von Spanien, Frankreich, Italien, FRONTEX und der Europäischen Fischereiaufsichtsagentur. Die Kommission hat bereits angekündigt, die Richtlinie über den Einsatz von SAFESEANET 2013 überarbeiten zu wollen, um SAFESEANET in EUROSUR einzugliedern.

e-Maritime

Die „e-Maritime"-Initiative der EU zielt darauf ab, durch finanzielle Unterstützung der Entwicklung und Akzeptanz neuester IKT-Basistechnologien den Einsatz fortgeschrittener Informationstechnologien im Seeverkehr zu fördern und damit die Seeverkehrsdienstleistungen zu verbessern. Besonders in den Häfen werden für die Erfassung von Informationen über Schiff, Ladung, Besatzung usw. zahlreiche und jeweils unterschiedliche automatisierte Informationssysteme verwendet. „Durch die e-Maritime-Initiative der EU soll Interoperabilität im weiteren Sinne gefördert werden. Ziel ist es, kohärente, transparente, effiziente und einfache Lösungen anzuregen, um die Zusammenarbeit, Interoperabilität und Einheitlichkeit zwischen den Mitgliedstaaten und Verkehrsunternehmen zu fördern.[62]

e-Zoll

Das „e-Zoll"-Projekt der EU hat das Ziel, alle papiergestützten Zollverfahren durch EU-weite elektronische Verfahren zu ersetzen. Damit soll sowohl die Sicherheit an den Außengrenzen der EU erhöht als auch der Handel vereinfacht werden. Das Projekt dient somit den Unternehmen und den Bürger/-innen gleichermaßen.[63] Eingeführte Zollinformationssysteme sind z. B. das EU-Zollinformationssystem, ein neues EDV-gestütztes Versandsystem, ein automatisiertes Ausfuhrsystem und ein System zur Registrierung und Identifizierung von Wirtschaftsbeteiligten.

Initiativen zur Bekämpfung des Drogenhandels und der Hochsee-Piraterie

Die Mitgliedstaaten haben zwei Arbeitsgruppen zur Bekämpfung des Drogenhandels über den Seeweg eingerichtet. Das Operations- und Analysezentrum zur Drogenbekämpfung im Atlantik (Maritime Analysis and Operation Centre–Narcotics) wurde 2007 von Spanien, Frankreich, Irland, Italien, den Niederlanden, Portugal und dem Vereinigten Königreich ins Leben gerufen, um „die polizeiliche Erkenntnisgewinnung zu verbessern und Polizeieinsätze auf hoher See zu koordinieren, um mit Kokain und Cannabis beladene Schiffe abzufangen". Marinebehörden und Strafverfolgungsorgane (Polizei, Zollbehörden) arbeiten mit dem Zentrum zusammen.[64] Das Koordinationszentrum zur Drogenbekämpfung im Mittelmeer (Centre de Coordination pour la Lutte Anti-Drogue en Méditerranée) ist eine Gesetzesvollzugsinitiative zur Eindämmung des Drogenschmuggels im westlichen Mittelmeerraum und wurde 2008 unter der französischen Ratspräsidentschaft gegründet. Alle EU-Mitgliedstaaten und nordafrikanischen Länder der Region können es zum bilateralen Informationsaustausch mit dem Ziel der Bekämpfung des Drogenhandels nutzen.[65] Beide Einrichtungen werden im EUROSUR-Verordnungsvorschlag erwähnt.[66] Die Europäische Kommission hat zudem angedeutet, dass das „Lagebild" von EUROSUR für Initiativen zur Bekämpfung der Piraterie eingesetzt werden könnte. 2010 rief die EU das Programm für kritische Seeverkehrsrouten ins Leben und führte Pilotprojekte im Golf von Aden, im Bab el-Mandeb, in der Straße von Malakka und in Singapur durch. Im Rahmen des Programms sollen Gemeinschaftsschiffen, die durch pirateriegefährdete Gebiete fahren, Überwachungs- und Schutzmaßnahmen zur Verfügung gestellt werden.[67]

62 Siehe „e-Maritime", Europäische Kommission, abrufbar unter: http://ec.europa.eu/transport/maritime/e-maritime_en.htm.

63 Siehe „Elektronischer Zoll", Europäische Kommission, abrufbar unter: http://ec.europa.eu/taxation_customs/customs/policy_issues/electronic_customs_initiative/index_de.htm.

64 Siehe „Maritime Analysis and Operation Centre–Narcotics", Europäische Beobachtungsstelle für Drogen und Drogensucht, abrufbar unter: http://www.emcdda.europa.eu/about/partners/maoc.

65 SEK (2009) 1341 endgültig, S. 5.

66 Artikel 17, Verordnungsvorschlag.

67 Siehe „Building regional maritime capacities" („Aufbau regionaler Meereskapazitäten"), Europäischer Auswärtiger Dienst, abrufbar unter: http://eeas.europa.eu/piracy/regional_maritime_capacities_en.htm.

Nationale und durch den EDSB koordinierte Militäreinsatze

2006 startete die Europäische Verteidigungsagentur ihr Seeüberwachungsprojekt mit dem Ziel, „unter Zuhilfenahme bestehender Informationsaustauschsysteme zwischen Schifffahrts- und Seebehörden ein Netzwerk“ zu schaffen, um Doppelarbeit und die Nutzung verfügbarer Technologien, Daten und Informationen zu vermeiden; auf einfache, effiziente und kostengünstige Weise die Zusammenarbeit zwischen zivilen und militärischen Akteuren zu verbessern; und die Sicherheit zu fördern.[68] 2006 wurde im Rahmen des Seeüberwachungsprojekts eine Arbeitsgruppe zum Thema Meeresüberwachungsvernetzung eingerichtet. Diese arbeitet an „Interoperabilität zwischen Schifffahrts- und Seebehörden durch die Entwicklung vereinbarter Standards und Protokolle. Anstelle eines neuen Systems werden hierzu Gateways und bereits existierende Systeme genutzt.“ 2009 beauftragte die Europäische Verteidigungsagentur ein Expertengremium (Wise Pen Team) bestehend aus fünf pensionierten, mit drei Sternen dekorierten Admirälen aus fünf EU-Staaten damit, sich im Kontext der gemeinsamen Europäischen Sicherheits-und Verteidigungspolitik für die Überwachung der Meere auszusprechen.[69] Da das Militär mittlerweile immer mehr Polizeifunktionen übernimmt – wie z. B. Kampf gegen Drogenhandel, Piraterie und Terrorismus – ist es wahrscheinlich, dass das Militär zunehmend stärkeren Zugang zu Meeresüberwachungsinstrumenten wie EUROSUR fordern wird.

68 „Maritime surveillance“, Europäische Verteidigungsagentur, abrufbar unter: http://www.eda.europa.eu/otheractivities/maritimesurveillance.

69 Wise Pen Team, „Maritime surveillance“ („Meeresüberwachung”); siehe auch Wise Pen Team, „Maritime surveillance in support of CSDP: The Wise Pen Team Progress Report“, Dez. 2010.

2.2 Die EU-Initiative für „intelligente Grenzen“

Im Gegensatz zu EUROSUR liegen für die EU-Initiative für „intelligente Grenzen“ bisher noch keine Gesetzesvorschläge vor. Es ist daher schwieriger, diese Initiative zu bewerten, da das Einreise-/Ausreisesystem und das Registrierungsprogramm für Reisende hinsichtlich ihres genauen Zwecks sowie ihrer Einrichtung, Funktion und Modalitäten nicht gründlich beschrieben sind. In diesem Kapitel gehen wir kurz auf die Entstehung der Initiative ein und heben bestimmte Aspekte hervor, die in den endgültigen Legislativvorschlag Aufnahme finden könnten und daher näher untersucht werden sollten.

Die Idee für ein europäisches Einreise-/Ausreisesystem, angelehnt an das US-VISIT-System, kam zuerst im Dezember 2004 auf. Damals legte das European Policy Evaluation Consortium seine ausführliche Folgenabschätzung des (damals) künftigen Visa-Informationssystems (VIS) vor.[70] Das EES wurde als computergestütztes System konzipiert, mit dessen Hilfe die Reisebewegungen aller Visuminhaber im Auge behalten werden können – von der Beantragung des Visums über die Einreise an der Außengrenze bis hin zur letztendlichen Ausreise aus dem Schengen-Raum. Die Identität aller Drittstaatenangehörigen sollte überprüft werden, biometrische Daten sollten jedoch nur von visumpflichtigen Drittstaatenangehörigen verlangt werden. Diese Daten sollten von den jeweiligen konsularischen Vertretungen erhoben und bei Einreise des Visuminhabers in die EU verifiziert werden. Gleichzeitig würde überprüft, ob es sich um die richtige Person handelt und ob er/sie einen terroristischen oder kriminellen Hintergrund hat. Bei Verlassen des Landes sollte der Visuminhaber die Ausreise an speziell dafür vorgesehenen „Exit Points“ bestätigen. Dies würde das Erfüllen der Einreisebestimmungen anzeigen und zukünftige Reisen erleichtern, jedoch gleichzeitig auch Personen ausfindig machen, die ihre genehmigte Aufenthaltsdauer überschritten haben (Overstayer). In diesem damaligen Konzept bestand keine Verbindung zwischen dem EES und dem RTP. In der Folgenabschätzung von 2004 wurde zu bedenken gegeben, dass ein solches System äußerst kostspielig wäre, erhebliche Beeinträchtigungen der Menschenrechte zur Folge hätte und „weit über das Ziel der besseren Umsetzung einer gemeinsamen Visumpolitik durch verbesserten Informationsaustausch zwischen Mitgliedstaaten, und auch über andere durch den Rat festgelegten Ziele für ein VIS, hinausschießen würde“.[71]

Die Schaffung eines biometrischen Visa-Informationssystems wurde beschlossen, und das Konzept für ein EES blieb von untergeordneter Priorität – nicht zuletzt deshalb, weil laut der Kommission die „für die innere Sicherheit und [die] für Ermittlungen zuständigen Stellen“ in Bezug auf das VIS einige Mängel festgestellt hatten: Das VIS erfasste nur DSA auf der sogenannten „schwarzen Liste“, die der Visumpflicht unterworfen sind. Es bestand kein vergleichbares Instrument zur Überprüfung der Identität oder der Rechtmäßigkeit der Einreise bei anderen Kategorien von DSA, wie beispielsweise bei Inhabern von Visa für den langfristigen Aufenthalt, bei Personen mit Aufenthaltstiteln oder bei nicht der Visumpflicht unterworfenen DSA (Personen auf der sogenannten „weißen Liste“).[72] Unter dem VIS konnte zudem die Einreise von DSA im Besitz eines Visums nicht überwacht werden. Auch

70 European Policy Evaluation Consortium, „Study for the extended impact assessment of Visa Information System“ („Studie über die ausführliche Folgenabschätzung des Visa-Informationssystems“), Dez. 2004.

71 Ebd., S. 31–37.

72 Die Länder auf der „schwarzen“ bzw. „weißen Liste“ werden in der Verordnung (EG) 539/2011 aufgeführt.

wurde nicht verzeichnet, ob sie vor Ablauf ihres Aufenthaltsrechts auch tatsächlich ausreisen.[73] Im Jahr 2005 schlug die Kommission vor, das EES außerdem als Register für Saisonarbeitnehmer/-innen aus Drittländern einzusetzen, um nachzuverfolgen, ob die DSA nach Ablauf ihrer temporären Aufenthalts-/Arbeitserlaubnis die EU tatsächlich verlassen haben oder aber ihre genehmigte Aufenthaltsdauer überzogen haben.[74] Es wurde jedoch auch zunehmend ersichtlich, dass die Erhebung von biometrischen Daten aller DSA, die in den Schengen-Raum einreisen, längere Wartezeiten an den Grenzen nach sich ziehen würde. Die Einrichtung eines EES wurde deshalb an die Einführung einer Regelung zur Erleichterung des Grenzübergangs für häufig die Grenze überschreitende Personen gekoppelt. Ende 2006 ersuchte der Europäische Rat die Kommission, vor Ende 2007 über die „Möglichkeiten einer Verbesserung der Zugangskontrolle zu berichten, darunter auch über die Durchführbarkeit eines allgemeinen automatischen Einreise-/Ausreise-Erfassungssystems zu diesem Zweck", um die Grenzkontrolle zu verstärken und eine zuverlässige Personenidentifizierung zu ermöglichen.[75]

Im Februar 2008 gab die Kommission ihre Mitteilung über „intelligente Grenzen" heraus, in der drei mögliche Maßnahmen vorgestellt wurden, um die Sicherheit in der EU zu verbessern und gleichzeitig die Ein- und Ausreise für Drittstaatenangehörige zu erleichtern: (1) die Einrichtung eines Registrierungsprogramms für Reisende, um „Bona-fide"-Reisenden den Grenzübertritt zu erleichtern; (2) die Schaffung eines Einreise-/Ausreisesystems; und (3) die Einführung eines europäischen Systems zur elektronischen Erteilung von Reisebewilligungen (Electronic System of Travel Authorisation – ESTA).[76] Diese Dokumente, gemeinsam mit der zugehörigen Folgenabschätzung, sind diejenigen öffentlich zugänglichen Unterlagen, in denen der Einsatz und die potenziellen Funktionalitäten des Systems am detailliertesten beschrieben sind. Während der EU-Ratspräsidentschaften Frankreichs und Tschechiens wurde die Einrichtung eines EES als Priorität betrachtet und die entsprechenden Vorschläge wurden von der mit Grenzfragen befassten Arbeitsgruppe des Rates (Gruppe „Grenzen") begeistert aufgenommen.[77] 2009 erklärte die Kommission, sie sei dabei, eine weitere Folgenabschätzung sowohl für das EES als auch das RTP

73 KOM (2005) 597 endgültig, S. 6. Die Kommission betonte 2006, dass auch das SIS II kein ausreichender Ersatz für ein EES sein könne, da registrierte Warnhinweise in Bezug auf Drittstaatsangehörige „nur Personen [betreffen], denen die Einreise in das Schengen-Gebiet verweigert wird; dabei handelt es sich um eine sehr kleine Gruppe im Vergleich zu denjenigen, die durch ein Einreise-/Ausreisesystem erfasst werden" (KOM (2006) 402 endgültig, S. 6.).

74 KOM (2005) 669 endgültig, S. 10–11.

75 Dokument des Rates 16879/06, S. 9. Unter der portugiesischen Ratspräsidentschaft wurde auf informellen Sitzungen des Strategischen Ausschusses für Einwanderungs-, Grenz- und Asylfragen am 4./5. Sept. 2007 und des Rates „Justiz und Inneres" am 1./2. Okt. 2007 weiterführend über den Einsatz neuer Technologien zur Verstärkung des EU-Grenzschutzes debattiert.

76 KOM (2008) 69 endgültig, S. 4–5. Ein solches europäisches ESTA sollte ursprünglich nur für nicht visumpflichtige DSA gelten. Diese müssten vor Reiseantritt einen elektronischen Antrag stellen, dem Angaben zur Identifizierung des Reisenden sowie Pass- und Reisedaten beizufügen seien.

77 Die Gruppe „Grenzen" beriet 2008 und 2009 über die Vorschläge. Finnland, Ungarn, das Vereinigte Königreich, die Niederlande, Deutschland und die Slowakei legten der Arbeitsgruppe ihre nationalen EES- bzw. RTP-Entwürfe vor. Zudem wurden den Mitgliedern der Arbeitsgruppe zwei Fragebögen ausgeteilt: einmal bezüglich ihrer Meinung zu dem Bedarf an einem EES für DSA im Schengen-Raum und den entsprechenden Funktionen eines solchen Systems; und ein anderer zur Erhebung relevanter statistischer Daten. Zwischen dem 31 Aug. und dem 6. Sept. 2009 wurde eine „Datenerhebungsübung" vorgenommen, um vergleichbare Daten über die Ein- und Ausreise verschiedener Kategorien von Reisenden an unterschiedlichen Außengrenzen zu sammeln, damit die Kommission bis Beginn des Jahres 2010 einen Legislativvorschlag vorlegen konnte.

vornehmen zu lassen, und kündigte für „spätestens Mitte 2011“ einen Legislativvorschlag an. Bis 2015 sollten dann die Systeme in Betrieb genommen werden.[78] Die „Vorschläge für ein Einreise-/Ausreisesystem“ gekoppelt an ein Registrierungsprogramm für Reisende fanden auch in das Stockholmer Programm Einzug, mit dem erklärten Ziel, die Systeme „so bald als möglich“ in Betrieb zu nehmen.[79]

Trotz dieser festgelegten Ziele scheinen die Mitgliedstaaten zunehmend weniger Enthusiasmus dafür aufzubringen, ein weiteres groß angelegtes Informationsmanagementsystem auf den Gebieten Justiz und Inneres anzulegen. Grund ist vielleicht die Tatsache, dass der erwartete „Migrationsdruck“ im Zuge des ‚Arabischen Frühlings‘ nie eingetreten ist. Ein noch bedeutenderer Faktor ist jedoch die anhaltende Finanzkrise, die die nationalen und EU-Haushaltsbudgets verstärkt unter Druck setzt. Verschärft wird das Problem noch durch die Einführung des Schengener Informationssystems II (siehe Kasten 3), das sich als bedeutend kostspieliger herausgestellt hat als erwartet. Einige – jedoch bei Weitem nicht alle – Mitgliedstaaten waren zudem von Anfang an besorgt darüber, dass für Systeme von der Größenordnung eines EES oder RTP strenge Datenschutznormen nötig sind, und wussten, dass dies für das Europäische Parlament eine heikle Angelegenheit ist. All dies wurde im Juli 2011 auf einer informellen Tagung des EU-Rates „Justiz und Inneres“ in Sopot (Polen) von den zuständigen Minister/-innen zur Kenntnis genommen, die erklärten: „Bevor neue Projekte wie dieses in Angriff genommen werden, müssen die Kommission und die Mitgliedstaaten zunächst sicherstellen, dass alle Beteiligten gleichermaßen bereit sind, gemeinsam auf die vereinbarten Ziele hinzuarbeiten. Die Minister/-innen werden daher aufgefordert, sich dazu zu äußern, ob das System ihrer Ansicht nach gerechtfertigt ist, insbesondere bezüglich eines Mehrwerts in Anbetracht der technischen Implikationen (z. B. Datenschutz) und der Kosten.“[80] Die Kommission wurde dann ersucht, eine weitere Mitteilung vorzulegen, in der diese Diskussionsbeiträge „reflektiert“ würden.

In ihrer Mitteilung zu "intelligenten Grenzen" vom Oktober 2011 stellte die Europäische Kommission einige Handlungsoptionen vor, machte jedoch gleichzeitig deutlich, dass „etwaigen künftigen Vorschlägen, die jeweils von einer umfassenden Folgenabschätzung begleitet wären, keinesfalls vorgegriffen werden [solle]“. Zwei Dinge standen jedoch fest. Erstens, dass die neue Europäische Agentur für das Betriebsmanagement von IT-Großsystemen die Verantwortung für die Entwicklung und das Betriebsmanagement der Systeme tragen würde, „um eine größtmögliche Qualität zu erreichen und Risiken, wie sie bei der Entwicklung des SIS II und des VIS zutage getreten sind, auf ein Minimum zu reduzieren“.[81] Zweitens, dass das europäische System zur elektronischen Erteilung von Reisebewilligungen für von der Visumpflicht befreite Drittstaatenangehörige nicht mehr zur Diskussion stand (weshalb es auch in diesem Bericht nicht weiter erwähnt wird), weil der potenzielle Sicherheitsgewinn für die Mitgliedstaaten „weder eine derart umfangreiche Erhebung personenbezogener Daten noch die finanziellen Kosten und die zu erwartenden Auswirkungen auf die internationalen Beziehungen rechtfertigen würde“.[82] Und im Februar 2012 fand unter der

78 SEK (2010) 1480 endgültig, S. 13.

79 Dokument des Rates 16484/09, S. 55.

80 Schlussfolgerungen der informellen Tagung der Minister/-innen für Justiz und Inneres in Sopot, 18./19. Juli 2011, S. 2.

81 KOM (2011) 680 endgültig, S. 13.

82 Ebd., S. 7. Dies könnte sich in Zukunft allerdings ändern. Erst vor Kurzem hat der deutsche Innenminister wieder Interesse an einem europäischen ESTA anstelle eines EES bekundet. Frankfurter Rundschau, EU-

dänischen Ratspräsidentschaft eine Konferenz zum Thema „Innovativer Grenzschutz“ statt, die Ergebnisse an die Kommission liefern sollte, welche wiederum bis Juni 2012 ihren Legislativvorschlag für "intelligente Grenzen" vorzulegen plante. Zum Zeitpunkt dieses Berichts erscheint es eher unwahrscheinlich, dass der Vorschlag vor Sommer 2012 vorgelegt wird.

2.2.1 Einreise-/Ausreisesystem

Mit dem Einreise-/Ausreisesystem sollen Overstayer ausfindig gemacht werden. Dabei handelt es sich um Personen, die mit einem gültigen Reisedokument und/oder Visum legal in die EU eingereist, aber nach Ablauf ihrer gesetzlichen Aufenthaltsberechtigung zu „illegalen Migrant/-innen“ geworden sind. Sie sollen die größte Gruppe „illegaler Einwanderer in der EU“ ausmachen.[83] In ihrem „Grenzschutzpaket“ von 2008 hatte die Kommission erklärt, mit dem EES würden automatisch Ort und Zeit der Ein- und Ausreise von Drittstaatenangehörigen registriert, denen ein Kurzaufenthalt (von bis zu drei Monaten) bewilligt wurde. So könnte man ihre Ausreise verifizieren bzw. sie ausfindig machen, wenn sie ihre genehmigte Aufenthaltsdauer überziehen.[84] In diesem Fall würde automatisch eine Warnmeldung an die zuständigen Behörden geschickt, wenn die autorisierte Aufenthaltsdauer einer Person abgelaufen ist und keine Ausreisedaten durch das EES erfasst worden sind.[85] Daraufhin könnten die nationalen Behörden nicht näher beschriebene „entsprechende Maßnahmen“ treffen, wie z. B. Geldbußen oder eine Ausweisungsverfügung. Die Kommission argumentierte, dass das EES Drittstaatenangehörige davon abschrecken würde, den autorisierten Aufenthalt zu überziehen, und dass ein solches System zweierlei Informationen liefern könnte: „für operationale Zwecke“ Informationen über einschlägige Muster (z. B. Reiserouten, in betrügerischer Absicht ausgestellte Einladungen, Herkunftsland und Reisegründe) sowie für visumpolitische Zwecke Daten über Migrationsströme und Overstayer.[86]

Bisher ist noch nicht klar, welche Daten durch das EES möglicherweise erhoben werden. Um seinem Zweck gerecht zu werden, nämlich dem Aufspüren von Overstayern durch Berechnen der in dem entsprechenden Gebiet verbrachten Zeit, müsste das System mindestens folgende Informationen

---

Innenminister beraten über Salafisten, 18. Mai 2012, abrufbar unter: http://www.fr-online.de/politik/g-6-treffen-in-muenchen-eu-innenminister-beraten-ueber-salafisten,1472596,16066774.html

83 KOM (2008) 69 endgültig, S. 5. Zwar liegen laut der Kommission keine verlässlichen Daten über die Gesamtzahl der irregulären Zuwanderer in die EU vor, aber vorsichtigen Schätzungen zufolge liegt sie zwischen 1,9 und 3,8 Millionen. KOM (2011) 680 endgültig, S. 4.

84 Derzeit ist das Abstempeln des Reisedokuments die einzige Möglichkeit, die Grenzschutzbeamte und Einwanderungsbehörden haben, um das Datum der Ein- und Ausreise zu vermerken. Diese Stempel sind offenbar „häufig schwer zu interpretieren“ und „manchmal ... unlesbar oder ... können das Ziel von Fälschungen sein“. SEK (2008) 153 endgültig, S. 10.

85 KOM (2008) 69 endgültig, S. 7. Die Kommission betonte 2011, dass die elektronische Erfassung der Ein- und Ausreiseinformationen im Idealfall zentral erfolgen sollte und nicht in den einzelnen Mitgliedstaaten. „Wenn diese Einreise- und Ausreiseinformationen zunächst auf nationaler Ebene erfasst würden, müssten sämtliche Informationen erst in mindestens 27 anderen nationalen Systemen repliziert werden, um sämtliche Ein- und Ausreisedaten aller Systeme auf dem aktuellen Stand zu halten. Bei Personen, die über einen anderen Mitgliedstaat aus dem Schengen-Raum ausreisen als über denjenigen, über den sie eingereist sind, könnte dies einen erheblichen Arbeits- und Zeitaufwand mit sich bringen“ (KOM (2011) 680 endgültig, S. 8.).

86 KOM (2008) 69 endgültig, S. 8.

aufzeichnen und speichern: (a) Grenzübergangsstelle bei Ein- und Ausreise; (b) Datum und Uhrzeit der Ein- bzw. Ausreise; (c) Art der Reisedokumente, einschließlich Dokumentnummer und Ausstellungsland; (d) die persönlichen Angaben über den Reisenden wie z. B. Name, Geschlecht und Geburtsdatum. Diese müssten dem Reisedokument entnommen werden.

In ihrer letzten Mitteilung zu „intelligenten Grenzen" aus dem Jahr 2011 erklärte die Kommission, es wäre „am besten", das EES phasenweise einzuführen und zunächst nur mit alphanumerischen Daten (z. B. Name, Staatsangehörigkeit, Passnummer) zu arbeiten und zu einem späteren Zeitpunkt biometrische Identifikatoren (Fingerabdrücke, digitales Gesichtsbild) einzuführen.[87] Allerdings hatte die Mehrheit der Mitgliedstaaten, die auf einer Ratstagung im Dezember 2011 Position bezogen, den Wunsch geäußert, die Erhebung biometrischer Daten im Rahmen des EES von Anfang an vorzunehmen.[88] Unklar ist, wie lange diese Daten aufbewahrt würden. Aus bisher geführten Diskussionen geht hervor, dass es sich um einen Zeitrahmen von sechs Monaten bis fünf Jahren (VIS-Standard) handeln könnte. Die Daten eines DSA, der regelgerecht in das Hoheitsgebiet ein- und wieder aus ihm ausgereist ist, werden wahrscheinlich für diesen Zeitraum aufbewahrt, um das Erkennen und Aufzeichnen von „Reisebewegungen" zu ermöglichen. Es bleibt abzuwarten, inwiefern sich die längerfristige Speicherung von Daten mit dem Grundsatz der Zweckbindung vereinbaren lässt, einem der Grundprinzipien des EU-Datenschutzrechts. 2008 sah die Kommission außerdem „ein automatisches Bereinigungsverfahren vor, welches alte Aufzeichnungen, die eine bestimmte Zeit lang gespeichert waren, löscht".[89]

Die Kommission hat ausdrücklich erklärt, dass die „mit dem Einreise-/Ausreisesystem gewonnenen Daten ... von den zuständigen Einwanderungsbehörden genutzt [würden]".[90] In der dazugehörigen Folgenabschätzung sieht die Kommission die Möglichkeit vor, auch anderen Behörden Zugriff auf die Datenbank mit Informationen über Overstayer zu gewähren: „verschiedene Behörden können, je nach vereinbartem Rechtsrahmen und wo nötig, auf die Informationen über die verschiedenen Zielgruppen in der Datenbank zugreifen und diese nutzen". Dies gilt jedoch nur „unter besonderen Umständen, wenn ordnungsgemäß bevollmächtigte Strafverfolgungsbehörden aus gutem Grund Nachweise über die bisherigen Reisebewegungen namentlich genannter Einzelpersonen benötigen".[91] Allerdings scheint es der Wunsch einiger Mitgliedstaaten zu sein, den Strafverfolgungsbehörden erweiterten Zugang zu der Datenbank zu gewähren.[92] Aktuell führen elf Mitgliedstaaten nationale Einreise-/Ausreisesysteme ein, und mindestens sieben von ihnen – Bulgarien, Zypern, Estland, Lettland, Ungarn, die Slowakei und Polen – scheinen ihren Strafverfolgungsbehörden regelmäßig Zugriff auf das System zu gewähren. In ihren Augen dienen

87 KOM (2011) 680 endgültig, S. 9.
88 Dokument des Rates 17706/11, S. 2.
89 SEK (2008) 153 endgültig, S. 25.
90 Ebd., S. 57. Dies soll auch „Einwanderungs- und Grenzkontrollbehörden" einschließen.
91 Ebd., S. 27
92 Auf der EU-Konferenz zu innovativem Grenzschutz, die unter der dänischen Ratspräsidentschaft im Februar 2012 abgehalten wurde, forderte beispielsweise Estland, dass das EES „von allen Strafverfolgungsbehörden genutzt werden sollte, die für Schmuggel, illegale Einwanderung und grenzüberschreitende Kriminalität zuständig sind". Malta schlug vor, das „EES in andere nationale Systeme zum Gesetzesvollzug zu integrieren" und „sofortigen Zugriff" zu gewähren, da dies „Ermittlungen bei Straftaten erleichtern würde". Siehe hierzu auch die kürzlich erfolgte Tagung der Gruppe „Strafverfolgung", bei der gefordert wurde, „die gegenwärtige und künftige Ratspräsidentschaft anzuhalten, den Vollzugsbehörden so bald als möglich Zugang zum EES zu gewähren". Dokument des Rates 10825/12, 5. Juni 2012, unter 2.

alle EU-Systeme demselben Zweck.[93] Sollte das EES ausdrücklich als Instrument für die innere Sicherheit klassifiziert werden, so ist es wahrscheinlich, dass eben diese Staaten fordern werden, ähnliche Daten wie die des Visa-Informationssystems ebenfalls aufzunehmen,[94] beispielsweise die Adresse des Unterkunftsgebers bzw. den Wohnort, den endgültigen Bestimmungsort und den Grund der Reise bzw. des Aufenthalts.[95]

2.2.2 Bezug des EES zu bestehenden EU-Systemen: VIS und SIS II

Der ausdrückliche Zweck des EES hat bedeutende Auswirkungen auf den Aufbau des Systems und seinen Bezug zu anderen EU-Datenbanken zur Rechtsdurchsetzung und Migrationskontrolle. Dies gilt insbesondere für das Visa-Informationssystem und das Schengener Informationssystem (SIS), das seit über einem Jahrzehnt von den Mitgliedstaaten und der Kommission überarbeitet wird (zu SIS II – siehe Kasten 3).

Da ein EES die Ein- und Ausreisedaten aller Drittstaatenangehörigen erfassen würde, ist es nur logisch, dass Informationen bezüglich visumpflichtiger DSA mit dem VIS-System interoperabel wären.[96] Nach Meinung der Kommission ist ein vollständig entwickeltes, betriebsbereites VIS sogar „Voraussetzung für ein System zur intelligenten Grenzverwaltung".[97] Wenn das EES lediglich dazu dienen soll, Overstayer auszumachen, so ist es am wahrscheinlichsten, dass eine eigene EES-Datenbank eingerichtet wird, die mit VIS und SIS (II) interoperabel ist und über eine eigene zentrale Systemarchitektur verfügt. Die biometrischen Merkmale des EES werden über das biometrische Abgleichsystem der Europäischen Union in die VIS-SIS-II-Systemarchitektur integriert werden, da die Kommission das biometrische Abgleichsystem als „zentrales Instrument zur biometrischen Identitätssicherung" für alle ihre europaweiten Anwendungen vorsieht. Somit können die biometrischen Daten der VIS-Datenbank mit an Grenzübergängen abgegebenen Fingerabdrücken abgeglichen werden.[98]

Zusätzlich zu der Überprüfung von Fingerabdrücken durch Anwendungen wie VIS wird im Rahmen des biometrischen Abgleichsystems auch eine Identifikation von Fingerabdruckdaten möglich sein, also das Durchsuchen umfangreicher Datensätze. In einem solchen Fall müssten nur die Daten und Orte der Ein- und Ausreise von visumpflichtigen Drittstaatenangehörigen erhoben werden, ohne dass die im VIS-System gespeicherten Information reproduziert werden müssen. Die personenbezogenen Daten sowie die Informationen über Ein- und Ausreisebewegungen nicht visumpflichtiger DSA würden in dieser separaten Datenbank gespeichert.[99] Ein eindeutiger Bezug zu

93 Laut der Kommission führen derzeit elf Mitgliedstaaten ein nationales EES ein (Finnland, Estland, Lettland, Litauen, Polen, die Slowakei, Ungarn, Rumänien, Bulgarien, Zypern und Portugal) (KOM(2011) 690 endgültig, S. 6.).

94 Artikel 9, VIS-Verordnung.

95 Dokument des Rates 13267/1/09 REV 1.

96 Dies scheint auch die von den Mitgliedstaaten bevorzugte Option zu sein. Dokument des Rates 17706/11, S. 2.

97 KOM (2011) 680 endgültig, S. 7.

98 Die Kommission erwähnte 2009 das EES in ihrer Informationsmanagement-Übersicht und erklärte, dass für ein EES „basierend auf der Verifizierung biometrischer Daten" dasselbe biometrische Abgleichsystem und dieselbe operative Ausrüstung wie für SIS II und VIS verwendet würden. Siehe Datenblatt zum biometrischen Abgleichsystem der Europäischen Union („European Union – Biometric Matching System"), abrufbar unter: http://www.nws-sa.com/biometrics/EU_Matching_CS.pdf.

99 Unter dem Grundsatz der Zweckbindung dürften im VIS-System keine Daten über nicht visumpflichtige DSA gespeichert werden.

dem VIS könnte auch auf andere Weise hergestellt werden. Sobald eine Person im EES als Overstayer vermerkt ist, könnte als mögliche Folge der nächste Visumantrag dieser Person für den Schengen-Raum abgewiesen werden – womit eine Bewilligung von Visumanträgen letztendlich implizit an die Bedingung geknüpft sein könnte, keinen Eintrag als Overstayer im System aufzuweisen.

Kasten3: Das Visa-Informationssystem und das Schengener Informationssystem/SIS II

Visa-Informationssystem

Das VIS ist seit dem 11. Oktober 2011 in Betrieb. In der zentralen VIS-Datenbank werden Daten über Visumanträge (auch abgelehnte Anträge) über einen Zeitraum von fünf Jahren gespeichert. Für Personen, die zum ersten Mal ein Visum beantragen (z. B. bei dem Konsulat eines Schengen-Staats), werden zudem zehn Fingerabdrücke und ein Digitalbild abgespeichert. Die ersten konsularischen Vertretungen, die dem System angeschlossen wurden, waren die in Algerien, Ägypten, Libyen, Mauretanien, Marokko und Tunesien, gefolgt von Israel, Jordanien, Libanon und Syrien. An den Außengrenzen des Schengen-Raums werden dann die Fingerabdrücke des Visuminhabers überprüft, um seine Identität zu verifizieren. Das Betriebsmanagement des VIS wird nach einer Übergangsphase von der neuen EU-Agentur für das Betriebsmanagement von IT-Großsystemen (die offiziell im Herbst 2012 die Arbeit aufnimmt) übernommen werden. Die zentrale Datenbank soll schlussendlich bis zu 80 Millionen Visumanträge umfassen. Neben den für Visumanträge zuständigen Behörden der Schengen-Staaten könnten künftig auch Asylbehörden – und in manchen Fällen auch EUROPOL und nationale Strafverfolgungsbehörden – zwecks Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger Straftaten Zugang zu den VIS-Daten erhalten. Die Kommission hat eingeräumt, dass es sinnvoll wäre, vor Einführung des EES in der Praxis die „vollständige und erfolgreiche Anwendung“ des VIS in allen konsularischen Vertretungen und Grenzübergangsstellen abzuwarten.

Schengener Informationssystem

Das SIS ist seit 1995 in Betrieb und mittlerweile in allen EU-Mitgliedstaaten außer Bulgarien und Rumänien eingeführt worden. Auch Norwegen, Island und die Schweiz haben es nicht umgesetzt. Unter dem Schengener Abkommen von 1990 schreiben die Vertragsstaaten Personen aus („Ausschreibung“), wenn um deren Festnahme ersucht wird (Art. 95) oder sie Gegenstand polizeilicher Ermittlungen (Art. 99) oder eines Strafverfahrens (Art. 98) sind; außerdem „Drittausländer“, denen die Einreise in den gesamten Schengen-Raum zu verweigern ist (Art. 96); und sie erlassen eine Sachfahndungsnotierung für gestohlene oder abhanden gekommene Kraftfahrzeuge, Feuerwaffen, Identitätspapiere und Banknoten (Art. 100). Daten zur Ausschreibung von Personen werden nicht länger als zehn Jahre gespeichert, müssen aber alle drei Jahre von der ausschreibenden Vertragspartei auf die Erforderlichkeit der weiteren Speicherung hin geprüft werden.[100] Grenzschutz- und Einwanderungsbeamte prüfen dann, ob Personen, die in den Schengen-Raum einreisen, im SIS (dem System, mit dem die Reisedokumente bei der Einreise in den Schengen-Raum geprüft werden) ausgeschrieben sind. Auch Polizeibeamte des Schengen-Raums können auf das SIS zugreifen, um zu überprüfen, ob bestimmte Personen in anderen Mitgliedstaaten gesucht werden. Es ist jedoch an den Mitgliedstaaten zu entscheiden, welche nationalen Organe (begrenzten) Zugang zu den im SIS vermerkten Ausschreibungen haben. In das SIS werden unter anderem folgende Informationen aufgenommen: Name, Künstlername, körperliche Merkmale, Geburtsort und -datum, Staatszugehörigkeit und ob die Person bewaffnet und/oder gewalttätig ist. Aus einer Ausschreibung geht hervor, welche Maßnahmen gegen die jeweilige Person ergriffen werden sollen; in den allermeisten Fällen handelt es sich um Drittstaatenangehörige, denen die Einreise in den Schengen-Raum zu verweigern ist. Werden die

100 Ausschreibungen gemäß Artikel 99 müssen allerdings jährlich überprüft werden. Daten in Bezug auf ausgestellte Identitätspapiere und Registriergeld werden nicht länger als fünf Jahre und Daten in Bezug auf Kraftfahrzeuge, Anhänger und Wohnwagen nicht länger als drei Jahre nach der Aufnahme gespeichert (Artikel 112–113, Schengener Abkommen).

Daten einer ausgeschriebenen Person oder eines Gegenstandes, nach dem gefahndet wird, in das SIS eingegeben, so liefert das System einen „Treffer“. 2010 produzierten insgesamt 35,69 Millionen Einträge mehr als 91.000 Treffer. Von 1991 bis 2010 wurde insgesamt 253.640 DSA wegen im SIS gespeicherter Daten die Einreise in das EU-Gebiet verweigert.

SIS II

Die Entwicklung und Umsetzung des Schengener Informationssystems der „zweiten Generation“ (SIS II) hat mit vielen Problemen zu kämpfen. Das neue System soll eine Erweiterung der Kapazitäten und Funktionalitäten des SIS bedeuten, indem zusätzliche Informationskategorien und biometrische Daten (wie z. B. Fingerabdrücke) aufgenommen werden. Das SIS II wird dasselbe biometrische Abgleichsystem verwenden wie das VIS. Die ersten offiziellen Tests des zentralen SIS II wurden im Mai 2011 aufgenommen; dennoch ist noch unklar, wann die EU-Mitgliedstaaten in das neue System eingebunden werden. Im Januar 2012 erklärte die Kommission, dass sich ihre Haushaltsverpflichtungen für die zentrale SIS-II-Architektur auf mehr als 135 Millionen Euro belaufen.[101] Auch die ausufernden Kosten für die Aufrüstung nationaler SIS-Systeme wird mit großer Sorge betrachtet.[102]

Klärungsbedarf besteht zudem bei der Frage, welche Beziehung zwischen dem SIS/SIS II und dem geplanten EES bestehen soll. Wenn das EES automatisch eine Warnmeldung an die Behörden eines Mitgliedstaates senden soll, sobald eine Person ihre gültige Aufenthaltsdauer überschritten hat und nicht ausgereist ist, dann erscheint es nur logisch, dies über das Schengener Informationssystem zu tun – welches in der Praxis den Polizeibehörden der Schengen-Staaten Zugriff auf die internationalen Ausschreibungen anderer beteiligter Staaten ermöglicht. Ohne eine solche automatische Verbindung zwischen dem EES und dem SIS/SIS II könnten Overstayer (besonders solche, die in einen anderen Mitgliedstaat ziehen) erst dann ausgemacht werden, wenn sie versuchen, den Schengen-Raum zu verlassen – was die Begründung für die Einrichtung eines EES-Systems zu Überwachungszwecken ziemlich untergraben würde. Allerdings wäre es gesetzwidrig, automatische Warnhinweise zu Overstayern über das SIS/SIS II herauszugeben und der Polizei routinemäßig Zugang zu diesen Daten zu gewähren, solange der entsprechend anwendbare Rechtsrahmen nicht erheblich abgeändert wird. Aus Artikel 24 der Verordnung (EG) Nr. 1987/2006 über SIS II geht eindeutig hervor, dass „Daten ... zur Einreise- oder Aufenthaltsverweigerung ... aufgrund einer nationalen Ausschreibung eingegeben [werden], die *auf einer Entscheidung der zuständigen Verwaltungsbehörden oder Gerichte beruht*, ... [welche] auf die Gefahr für die öffentliche Sicherheit oder Ordnung oder die nationale Sicherheit gestützt wird“. Solange die SIS-Verordnung also nicht abgeändert wird, können Overstayer nicht im SIS vermerkt werden (lediglich die resultierende Ausweisungsverfügung, wenn eine Abschiebungsanordnung vorliegt).[103] Das ‚Meijers Committee‘ („Ständiger Expertenausschuss zu Fragen des internationalen Einwanderungs-, Flüchtlings- und Strafrechts“) hat überdies darauf aufmerksam gemacht, dass die SIS-II-Verordnung derzeit daran „zweifeln lässt“, ob die Ausschreibung von Personen mit Einreiseverbot im SIS rechtens ist. Daher seien Änderungen nötig,

101 KOM(2011) 907 endgültig, S. 8

102 Siehe beispielsweise Europäisches Parlament: Bericht über den Vorschlag für eine Verordnung des Rates zur Änderung des Beschlusses 2008/839/JI über die Migration vom Schengener Informationssystem (SIS 1+) zum Schengener Informationssystem der zweiten Generation (SIS II), A7-0127/2010 vom 29.04.2010.

103 Richtlinie 2008/115/EG des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über gemeinsame Normen und Verfahren in den Mitgliedstaaten zur Rückführung illegal aufhältiger Drittstaatsangehöriger [eigene Hervorhebung].

um das Verhältnis zwischen der aktuellen SIS-II-Verordnung und dem „Einreiseverbot“ aus der Rückführungs-Richtlinie (2008/115/EG) zu klären.[104]

2.2.3 Registrierungsprogramm für Reisende

Das RTP ist ein freiwilliges EU-Programm, das darauf abzielt, „Bona-fide-Reisenden“ einen möglichst schnellen Grenzübertritt zu ermöglichen. Die Teilnehmer/-innen dieses Programms müssten sich zunächst einem umfassenden Prozess der Vorabprüfung unterwerfen und kämen dann in den Genuss „vereinfachter und automatischer“ Grenzkontrollen. Die Kommission schätzt, dass durch das RTP „der Grenzübertritt von 4-5 Millionen Reisenden jährlich beschleunigt werden [könnte] und der Grundstein für weitere Investitionen in automatische Grenzkontrolltechnologien für die wichtigsten Grenzübergänge gelegt [würde]“.[105] Für registrierte Reisende könnte „die durchschnittliche Grenzübertrittsdauer von derzeit 1-2 Minuten auf unter 30 Sekunden gedrückt werden“.[106]

Ein solches freiwilliges Registrierungsprogramm für Reisende muss den zuvor zugelassenen Reisenden eine schnelle Einreise ermöglichen, um für potenzielle Teilnehmer/-innen interessant zu sein. Hierfür werden automatische Kontrollgates als die einzige Lösung angesehen. An diesen Gates würde ein automatisches Lesegerät die in den Reisedokumenten enthaltenen oder in einem System oder einer Datenbank gespeicherten biometrischen Daten lesen und sie mit den biometrischen Merkmalen des Reisenden (Fingerabdrücke und Gesichtsbild) abgleichen. Die Kommission argumentiert, dass ein RTP-System einen „effizienteren Einsatz“ von Grenzschutzbeamten bedeuten würde, da die automatischen Kontrollgates kaum oder gar nicht von Grenzschutzbeamten beaufsichtigt werden müssten. In ihrer Mitteilung von 2008 erklärte die Kommission, dass ein einziger Grenzposten womöglich für bis zu zehn automatische Kontrollgates zuständig sein könne.[107] Ein RTP sollte daher zumindest theoretisch dafür sorgen, dass Grenzposten anderweitig eingesetzt werden können und sich stärker auf „risikoreichere“ Reisende konzentrieren können, die nicht am RTP teilnehmen. Dies würde alle Reisenden faktisch in Personengruppen mit hohem und niedrigem Risikoprofil unterteilen. Zwar könnte jeder Drittstaatenangehörige auf dem Konsulat eines jeden Mitgliedstaats die Teilnahme an diesem Programm beantragen; doch gelockerte Grenzkontrollen würden nur für diejenigen Reisenden Realität, die als Reisende mit niedrigem Risikoprofil bzw. „Bona-fide-Reisende“ eingestuft werden und bei denen man davon ausgeht, dass sie keine Bedrohung für die Sicherheit der Mitgliedstaaten darstellen.

---

104 Meijers Committee: Note on the coordination of the relationship between the Entry Ban and the SIS-alert: an urgent need for legislative measures („Mitteilung zur Koordinierung der Beziehung zwischen dem Einreiseverbot und einer Ausschreibung im SIS: dringender Bedarf an rechtlichen Maßnahmen“), 8. Februar 2012, abrufbar unter: http://www.commissie-meijers.nl/assets/commissiemeijers/CM1203%20Note%20on%20the%20coordination%20of%20the%20relationship%20between%20the%20Entry%20Ban%20and%20the%20SIS-alert-%20An%20urgent%20need%20for%20legislative%20measures_COM.pdf

105 KOM (2011) 680 endgültig, S. 12.

106 Ebd.

107 Gleichzeitig räumte die Kommission ein, dass es in der Praxis „äußerst schwierig“ sei, die Folgen des EES und RTP für die eingesetzte Zahl an Grenzschutzbeamten und die Wartezeit der Reisenden abzuschätzen, „da diese Faktoren fast gänzlich von dem jeweiligen Grenzübergang abhängen und davon, ob das Registrierungsprogramm für Reisende bzw. das automatische Grenzkontrollsystem an diesem Grenzübergang eingesetzt wird oder nicht“ (SEK (2008) 153 endgültig, S. 34.).

Die Kommission nannte 2008 einige Kriterien, die eine/-n Reisende/-n mit niedrigem Risikoprofil ausmachen könnten. Als Bona-fide-Reisende wurden diejenigen Reisenden vorgeschlagen, die aus legitimen Gründen (beispielsweise als Geschäftsreisende) häufig in den Schengen-Raum reisen, ein verlässliches Reiseverhalten aufweisen (stets die an ihre Aufenthaltsdauer geknüpften Bedingungen respektieren),[108] einen Nachweis ausreichender Existenzmittel vorlegen können und im Besitz eines biometrischen Passes sind.[109] Es wird sichergestellt, dass die Reisenden auf keiner Beobachtungsliste stehen, d. h. dass sie keine Gefahr für die öffentliche Ordnung, innere Sicherheit, öffentliche Gesundheit oder internationalen Beziehungen einer der Mitgliedstaaten darstellen.[110] Laut Aussage der Kommission „können weitere Kriterien eingeführt werden".[111] In der Mitteilung der Kommission von 2011 fand der Prozess der Vorkontrolle weit weniger Berücksichtigung. So wurde lediglich festgehalten, sie „müsste so gründlich sein, dass die eigentlichen Kontrollen an der Grenze entschärft werden könnten".[112] Auf der informellen Ratstagung im Juli 2011 deutete der Rat an, die Auswahlkriterien unter Umständen den Bedingungen angleichen zu wollen, die Inhaber eines Mehrfachvisums erfüllen müssen.[113]

Die Kommission und Mitgliedstaaten möchten statt 27 dezentralen interoperablen Systemen lieber eine zentrale EU-weite RTP-Datenbank für DSA einrichten.[114] In der Mitteilung der Kommission von 2011 finden sich drei Möglichkeiten für die Speicherung der Daten von registrierten Reisenden zur automatischen Überprüfung ihrer Identität: (1) Speicherung der alphanumerischen und biometrischen Daten in einer zentralen Datenbank; (2) Speicherung der Daten auf einer dem Reisenden ausgestellten Marke („token"); (3) Kombinieren einer zentralen Datenbank mit einer Marke für den registrierten Reisenden, auf der lediglich eine nur einmal existierende Kennnummer (die Antragsnummer) gespeichert wäre.[115] Die dritte Option ist wohl die beste – hinsichtlich Datenschutz und -sicherheit –, aber auch teurer in der Entwicklung als ein einfaches zentrales Register (auf die Kostenfrage wird in Kapitel 4 näher eingegangen). Die meisten Mitgliedstaaten haben eine Präferenz für die zentrale Datenspeicherung signalisiert, einige ziehen jedoch eine Kombination aus zentraler Datenbank und Marke vor.[116]

Derzeit gibt es nur vier RTP, die an großen Flughäfen und Anschlussstellen der EU operativ sind: drei von ihnen (*ABG* in Deutschland, *Iris* im Vereinigten Königreich und *Privium* in den Niederlanden) arbeiten mit Iriserkennung, während *Parafes* in Frankreich Fingerabdrücke registriert. Weiterhin existieren drei Systeme mit automatischen Kontrollgates, die unabhängig von jeglichem RTP-System operieren, nämlich *RAPID* in Portugal und die Kontrollgate-Systeme im Vereinigten Königreich und in Spanien. Diese arbeiten alle mit Gesichtserkennung. Die meisten solcher Systeme stützen sich nur

108 Mit dieser Bedingung würde allerdings vorausgesetzt, dass ein funktionstüchtiges EES existiert (vgl. unten).
109 KOM (2008) 69 endgültig, S. 6.
110 Die Kommission sieht vor, dass auch EU-Bürger/-innen beim Überschreiten der Außengrenzen solche automatischen Kontrollgates nutzen könnten, „abgesehen davon, dass nach dem Schengener Grenzkodex nur stichprobenweise ein Abgleich mit dem SIS und nationalen Datenbeständen durchgeführt werden kann" (KOM (2008) 69 endgültig, S. 7.).
111 SEK (2008) 153 endgültig, S. 62.
112 KOM (2011) 680 endgültig, S. 11.
113 Schlussfolgerungen der informellen Tagung der Minister/-innen für Justiz und Inneres in Sopot, 18.-19. Juli 2011, S. 3.
114 KOM (2011) 680 endgültig, S. 8.
115 Ebd., S. 8–9.
116 Dokument des Rates 17706/11, S. 2.

auf einen einzigen biometrischen Identifikator, während das geplante EU-RTP allem Anschein nach sowohl mit Gesichts- als auch Fingerabdruckerkennung arbeiten wird. Die Teilnahme an RTPs innerhalb der nationalen Programme ist im Allgemeinen auf Bürger/-innen der EU/des EWR beschränkt, und sie sind nicht interoperabel. Viele Mitgliedstaaten haben angesichts der hohen Kosten und des begrenzten Mehrwerts für Länder mit nur wenigen Reisenden Bedenken, was die Notwendigkeit eines EU-weiten Registrierungsprogramms für Reisende angeht.[117]

117 Siehe auch die Reaktionen vieler Teilnehmer/-innen an der EU-Konferenz zu innovativem Grenzschutz in Dänemark im Februar 2012.

3 Auswirkungen der Initiativen EUROSUR und „Intelligente Grenzen“ auf die Grundrechte

Bei einer Analyse der Auswirkungen der Initiative „Intelligente Grenzen“ und des EUROSUR-Entwurfs auf die Grundrechte ist zu beachten, dass zwar bereits ein Legislativvorschlag zu EUROSUR einschließlich einer detaillierten Folgenabschätzung vorliegt, die Kommission aber noch keinen Beschluss über den genauen Aufbau und die Modalitäten des Smart Border-Pakets getroffen hat. In diesem Kapitel wird daher nur auf hervorstechende Merkmale dieser beiden Initiativen hingewiesen, die mögliche Verstöße gegen die grundlegenden Menschenrechte beinhalten.

Rechtsgrundlage von EUROSUR ist Artikel 77(2)(d) des Vertrags über die Arbeitsweise der Europäischen Union zur schrittweisen Einführung eines integrierten Grenzschutzsystems an den Außengrenzen. Die Entwicklung von EUROSUR ist bereits weit fortgeschritten. Wie die Kommission jedoch betont hat, kann mit der Entwicklung des Einreise-/Ausreisesystems und des Registrierungsprogramms für Reisende erst begonnen werden, „wenn das Europäische Parlament und der Rat die Rechtsgrundlage für die Systeme mit den genauen Spezifikationen erlassen haben“.[118] Auch die Initiative „Intelligenter Grenzen“ gründet sich auf Artikel 77 des Vertrags, jedoch vermutlich eher auf Artikel 77(2)(b), der Maßnahmen zur Einführung von Kontrollen erlaubt, denen Personen beim Überschreiten der Außengrenzen unterzogen werden. Sämtliche Vorlagen müssen gemäß dem ordentlichen Gesetzgebungsverfahren durch das Europäische Parlament und den Rat verabschiedet werden.

Die Europäische Kommission muss gewährleisten, dass sie in ihren Vorschlägen die Charta der Grundrechte berücksichtigt.[119] Auch die Mitgliedstaaten müssen bei der Umsetzung von Rechtsvorschriften die Charta einbeziehen.[120] Was die Menschenrechte angeht, gibt es bei beiden Vorschlägen starke Bedenken bezüglich des Schutzes personenbezogener Daten. Die Initiative „Intelligente Grenzen“ bedeutet wahrscheinlich die Schaffung zumindest einer zentralisierten EU-Datenbank mit biometrischen Daten, auf die eine derzeit unbekannte Anzahl von Akteuren wird zugreifen können. Der EUROSUR-Vorschlag hat dagegen nur minimale Auswirkungen auf den Datenschutz, weil das System keine personenbezogenen oder biometrischen Daten in größeren Mengen erfasst oder in einer zentralen Datenbank zusammenführt. Dennoch könnte die Einbeziehung zumindest einiger personenbezogener Daten in EUROSUR und den gemeinsamen Informationsraum im Allgemeinen sowie die mögliche Weitergabe personenbezogener Daten an Drittstaaten und deren Behörden künftig gegen den Datenschutz verstoßen. Beide Initiativen haben möglicherweise außerdem Auswirkungen auf das Recht auf Asyl. Und nicht zuletzt wird im EUROSUR-Vorschlag auch ausdrücklich als humanitäres Ziel die Rettung von Menschenleben genannt; ein Element, das, wie bereits erläutert, jedoch weiter gestärkt werden muss.

118 KOM (2011) 680 endgültig, S. 13.
119 Siehe KOM (2005) 172 endgültig, S. 3.
120 Siehe auch Präambel 6 des EUROSUR-Verordnungsvorschlags.

3.1 Recht auf Privatsphäre und Schutz personenbezogener Daten

Zum Schutz der nationalen oder öffentlichen Sicherheit und zur Verhinderung von Straftaten ist der Eingriff von staatlichen Organen in die unveräußerlichen Menschenrechte in bestimmten Fällen notwendig. Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte legt drei Bedingungen für derartige Eingriffe fest: sie müssen legal sein, ein rechtmäßiges Ziel verfolgen und in einer demokratischen Gesellschaft erforderlich sein.[121] Die Initiative „Intelligente Grenzen" und die Schaffung von EUROSUR verletzen das Recht auf Privatsphäre und den Schutz personenbezogener Daten in unterschiedlichem Maße. Die Erfassung und Verarbeitung personenbezogener Daten und insbesondere biometrischer Daten ist ein zentrales Merkmal der Initiative „Intelligente Grenzen"; sie spielt beim Aufbau von EUROSUR jedoch nur eine untergeordnete Rolle. Dennoch gibt es auch bei EUROSUR Bedenken hinsichtlich des Schutzes von Privatsphäre und Daten, insbesondere was den Einsatz von Drohnen und anderen Luftüberwachungssystemen angeht, die im derzeitigen Legislativvorschlag nicht angemessen behandelt werden.

3.1.1 EUROSUR

Die Kommission betont, dass EUROSUR nicht als System zur Regelung der Erhebung, der Speicherung oder des grenzüberschreitenden Austauschs personenbezogener Daten gedacht ist.[122] Der Schwerpunkt von EUROSUR liegt stattdessen in der Überwachung bestimmter geografischer Räume (Grenzen) und Aktivitäten (illegale Grenzüberschreitungen). Nach Angabe der Kommission werden „Lagebilder (…) grundsätzlich keine personenbezogenen Daten enthalten, sondern dienen vielmehr dem Austausch von Informationen über Vorfälle und Sachobjekte, zum Beispiel im Hinblick auf das Aufspüren und Verfolgen von Schiffen."[123] Artikel 8 des Entwurfs sieht außerdem vor, dass die Lagebilder der Agentur FRONTEX und der nationalen Koordinierungszentren vorwiegend Vorfälle, grenzüberschreitende Kriminalität und Krisensituationen, den Standort der nationalen Kräfte (zur Grenzsicherung) und strategische Informationen sowie Geodaten umfassen.

Allerdings sind derzeit neun nationale Koordinierungszentren (in Bulgarien, Zypern, Deutschland, Dänemark, Estland, Spanien, Rumänien, Slowenien und der Slowakei) ermächtigt, personenbezogene Daten zu verarbeiten und in ihre nationalen Lagebilder einzubeziehen.[124] Die Beschreibung der einzelnen „Schichten" der nationalen Lagebilder lässt außerdem darauf schließen, dass personenbezogene Daten unter bestimmten Umständen doch einbezogen werden können. Die vorgesehenen „Ereignisschicht"[125], in der Vorfälle im Zusammenhang mit illegalen Grenzübertritten oder Drogen- und Menschenschmuggel erfasst werden, könnte beispielsweise auch

121 Die Auslegung der Richtlinie 95/46/EG und der Verordnung (EG) Nr. 45/2001 ist zum Teil von der einschlägigen Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte abhängig, siehe beispielsweise Gerichtshof der Europäischen Gemeinschaften, Österreichischer Rundfunk u.a. (Verbundene Rechtssachen C- 465/00, C-138/01 und C-139/01, Urteil des Gerichtshofs vom 20. Mai 2003, Plenum, Slg. 2003, I-4989).

122 KOM (2011) 873 endgültig, S. 3.

123 Artikel 2, Verordnungsvorschlag.

124 SEC (2011) 1538 final, S. 31–32.

125 Artikel 9.3.a des Verordnungsvorschlags.

personenbezogene Daten zu Täter/-innen und Opfern enthalten. Und wenn ein verdächtigtes Schiff überwacht wird, dürften vermutlich auch Daten über Eigentümer/-innen, Reeder/-innen, Passagiere, Besatzung, Mittelsmänner und -frauen usw. verarbeitet werden. Der Verordnungsvorschlag enthält ferner die ziemlich vage Formulierung, dass die Ereignisschicht Daten zu „unbekannten und verdächtigen (…) Personen an den oder in der Nähe der Außengrenzen des betreffenden Mitgliedstaats" umfassen kann.[126] In die Einsatzschicht des nationalen Lagebilds können auch Informationen zu den an den Einsätzen beteiligten Behörden aufgenommen werden.[127] Die Analyseschicht des nationalen Lagebildes umfasst ein nachrichtendienstliches Informationsbild, das nicht näher bestimmte „Migrantenprofile" umfasst[128] und eine „Teilschicht Bildmaterial und Geodaten, die Bezugsbilder, Hintergrundkarten, Bewertungen aufgrund von validierten Informationen, Änderungsanalysen (Erdbeobachtungsbilder) sowie Veränderungserkennungsdaten, georeferenzierte Daten und Karten enthält, die die Durchlässigkeit der Grenzen zeigen".[129] Es steht zwar noch nicht fest, ob dazu auch Bilder erkennbarer Personen gehören, dies scheint jedoch mit größter Sicherheit der Fall zu sein.

Die nationalen Koordinierungszentren dürfen diese Daten zum Zweck der Erstellung eines europäischen Lagebilds an FRONTEX weitergeben,[130] es ist jedoch unklar, ob FRONTEX diese Daten im europäischen Lagebild verwenden darf. Die FRONTEX-Verordnung sieht vor, dass FRONTEX personenbezogene Daten zur Erstellung von Risikoanalysen im Rahmen gemeinsamer Aktionen, Pilotprojekte und Soforteinsätze „verarbeiten" kann, die Daten in den Ergebnissen der Risikoanalyse jedoch „anonymisiert" werden müssen.[131] Man könnte nun argumentieren, dass das europäische Lagebild und insbesondere die „Analyseschicht", die Risikoeinstufungstrends enthält, einer derartigen Risikoanalyse entsprechen. In der Begründung zur EUROSUR-Verordnung ist festgelegt, dass die Mitgliedstaaten personenbezogene Daten „in Ausnahmefällen" an FRONTEX weitergeben können und nationale Lagebilder, die derartige Daten enthalten, „nur zwischen benachbarten Mitgliedstaaten" ausgetauscht werden dürfen."[132] Für Fälle, in denen FRONTEX beispielsweise in der „Ereignisschicht" oder „Einsatzschicht" des europäischen Lagebilds personenbezogene Daten aufführt, sind keine entsprechenden Beschränkungen vorgesehen. Daher muss dringend der tatsächliche Umfang geklärt werden, in dem EUROSUR personenbezogene Daten verarbeitet. Dies betrifft insbesondere Artikel 10 des Verordnungsentwurfs.

Schließlich kann FRONTEX Daten von Satellitenbildern und Drohnen[133] im Rahmen der „gemeinsamen Anwendung von Überwachungsinstrumenten" nutzen, um den nationalen Koordinierungszentren und der Agentur Informationen über die Überwachung der Außengrenzen und im Grenzvorbereich zur Verfügung zu stellen.[134] Gemäß den Begriffsbestimmungen ist ein „Außengrenzabschnitt" die Land- oder Seeaußengrenze eines Mitgliedstaats gemäß den

126 Artikel 9.3.d [Hervorhebung der Autoren].
127 Artikel 9.5.b.
128 Artikel 9.6.c.
129 Artikel 9.6.d.
130 Laut Artikel 10.2.d kann FRONTEX zusätzliche Informationen aus „sonstigen Quellen" erhalten. Diese könnten auch personenbezogene Daten umfassen.
131 Artikel 11c.3.b. der Verordnung (EU) Nr. 1168/2011
132 KOM (2011) 873 endgültig, S. 2.
133 Artikel 12.3
134 Artikel 12.1

innerstaatlichen Rechtsvorschriften.[135] Der „Grenzvorbereich“ ist recht allgemein als das geografische Gebiet jenseits der Außengrenze von Mitgliedstaaten definiert, das nicht durch ein nationales Grenzüberwachungssystem erfasst ist. Die Folgenabschätzung bietet lediglich folgende negative Erklärung: Das Hoheitsgebiet der EU-Mitgliedstaaten assoziierter Länder liegt außerhalb des Anwendungsbereichs von EUROSUR.[136] Dieses Einsatzgebiet lässt viele Fragen bezüglich des Schutzes von Privatsphäre und personenbezogenen Daten offen, welche in der Verordnung nicht ausreichend behandelt werden.

Neben der Überwachung von Landaußengrenzen und Grenzvorbereichen werden im Rahmen der europäischen Initiative für eine Globale Umwelt- und Sicherheitsüberwachung (GMES) zwei weitere Szenarien für den Einsatz von Drohnen eingeführt: die Suche nach Schiffen auf hoher See und die Überwachung der Häfen und Küsten bestimmter benachbarter Drittstaaten.[137] Durch die Überwachung eines Hafens lässt sich feststellen, ob bzw. wann ein bestimmtes Schiff ablegt. Küsten „die weiter als 40 Seemeilen von der Küste eines EU-Mitgliedstaats entfernt sind (außerhalb der Reichweite von Küstenradarstationen) können mit Hilfe von Drohnen überwacht werden, um „Vorbereitungen“ zu erfassen, die auf illegale Grenzüberschreitungen hindeuten können, wie „beispielsweise der Aufbau von Zelten oder Hütten, Ansammlungen von Fahrzeugen oder Boote am Strand.“[138] Im Rahmen der GMES wird auch „der Einsatz von unbemannten Fluggeräten zur Erfassung, Klassifizierung und Identifizierung von zumindest 80 % aller Schiffe in einem vorab festgelegten Bereich (beispielsweise in Krisensituationen)“ erwogen. Laut Begründung des EUROSUR-Vorschlags könnte die gemeinsame Anwendung von Überwachungsinstrumenten „mit Unterstützung der einschlägigen europäischen Raumfahrtprogramme, darunter das operative Programm GMES (Globale Umwelt- und Sicherheitsüberwachung), eingeführt werden“ (siehe Kapitel 4).[139]

Derzeit lässt sich nicht sagen, ob die Drohnen, die im Rahmen von EUROSUR eingesetzt werden, Personen erkennen oder personenbezogene Daten verarbeiten und speichern können. FRONTEX hat zwar großes Interesse am Einsatz von Drohnen gezeigt, es muss sich aber erst noch zeigen, ob die Agentur eigene Drohnen anschaffen wird. Laut dem Arbeitsprogramm der Agentur FRONTEX für das Jahr 2012 führt die Forschungs- und Entwicklungsabteilung der Agentur derzeit eine neunmonatige Studie zur „Ermittlung kostengünstiger und effektiver Lösungen für Luftfahrzeugsysteme mit optionaler Bemannung für den Einsatz in gemeinsamen Aktionen von FRONTEX (zu Wasser und zu Land)“ durch.[140] Laut Arbeitsprogramm prüft das „Projekt für gemeinsame

135 Gemäß dem Schengener Grenzkodex sind „Außengrenzen“ die Landgrenzen (einschließlich der Fluss- und Binnenseegrenzen) und die Seegrenzen der EU-Mitgliedstaaten sowie die Flughäfen, die Flussschifffahrts-, See- und Binnenseehäfen, soweit sie nicht Binnengrenzen sind.

136 SEC (2011) 1538 final, S. 24.

137 SEC (2011) 145 final, S. 8. Die Europäische Initiative zur GMES wird von der Europäischen Kommission koordiniert und verwaltet. Gemäß dem rechtlichen Hinweis, der diesem Dokument zur GMES voransteht, gibt das Dokument nicht die Ansichten der Agentur FRONTEX oder der Europäischen Kommission wieder und darf „keinesfalls (...) als Vorschlag oder endgültige Spezifikation für künftige Einsatzdienste gewertet werden".

138 GMES CONOPS doc. Version 1.4, 7. Juli 2011, S. 11.

139 KOM (2011) 873 endgültig, S. 2. Die Kommission erwähnt GMES als „einschlägiges Programm“ für die Erbringung der Dienstleistungen für die gemeinsame Anwendung von Überwachungsinstrumenten. KOM (2011) 873 endgültig, S. 38.

140 Dokument des Rates 6514/12, S. 97.

Überwachungsinstrumente“ außerdem, ob FRONTEX Satellitenbilder und Schiffsmeldesysteme gemeinsam zur Grenzüberwachung nutzen kann, um dem EUROSUR-Netzwerk Überwachungsdaten zur Verfügung zu stellen. Auch dies „wird unter Verwendung von Maßnahmen der GMES (...) und in enger Zusammenarbeit mit EUSC und EMSA erfolgen.”[141]

Wenn man bedenkt, dass EUROSUR die „Grenzkontrollfunktion des gemeinsamen Informationsraums der EU“ übernehmen soll, ist die fehlende Klarheit bezüglich der Verarbeitung personenbezogener Daten inakzeptabel.[142] Wie in Kapitel 2.1.3 erläutert, besteht der CISE aus einem dezentralisierten Rahmen zum Informationsaustausch, der die relevanten Nutzergruppen verknüpft. Grundlage für den Informationsaustausch ist das Prinzip „Kenntnis nur, wenn nötig“ und die Notwendigkeit des Informationsaustauschs.[143] Zwar dürfte sich der Großteil der ausgetauschten Daten auf Identität und Kurs von Booten und Schiffen beziehen, es lässt sich aber nicht ausschließen, dass auch personenbezogene Daten über Besatzung und Passagiere weitergegeben werden.

Die Kommission betont die Notwendigkeit eines klaren Rechtsrahmens für den Austausch von Daten, „der mindestens die Art der betreffenden Daten sowie die Möglichkeiten und Rechte der Datenanbieter und -empfänger beim Datenaustausch, die Zwecke (und Methoden) des Austauschs festlegt und die nötigen Sicherheitsvorkehrungen für die Vertraulichkeit und Sicherheit von (bestimmten) Daten und gegebenenfalls den Schutz personenbezogener Daten einschließt.”[144] Laut Fahrplan werden diese Punkte jedoch erst geklärt, wenn die vorherigen Stufen für die Schaffung des gemeinsamen Informationsraums abgeschlossen sind. Zu diesem Zweck müssen die „Hindernisse für den Datenaustausch im EU-Recht herausgefiltert (...) und Möglichkeiten zu ihrer Beseitigung erforscht werden.“[145] Dies ist bedauerlich, da der gemeinsame Informationsraum durch die Menge der möglichen „Nutzergruppen“, zu denen Zoll, Grenzschutz, Strafverfolgungsbehörden und Streitkräfte gehören, aus Datenschutzgründen äußerst bedenklich ist. Der Datenschutz sollte daher bereits bei der Planung berücksichtigt und in den Aufbau des Systems integriert werden.[146] Die Kommission betont, dass „die Ebenen auf der Grundlage der anzuwendenden Rechtsinstrumente durch die jeweiligen Inhaber der entsprechenden Informationen auf Ebene der Mitgliedstaaten und der EU gemanagt werden. Somit werden die durch die Rechtsinstrumente festgelegten Befugnisse der nationalen Behörden ebenso wie die der EU-Stellen vollständig geachtet.“[147] Das bedeutet, dass Daten von EUROSUR beispielsweise in internationalen Strafverfolgungseinsätzen mit militärischen Mitteln (z. B. Einsätze im Kampf gegen Piraterie) verwendet werden könnten. Sofern Seestreitkräfte Maßnahmen zur Seeraumüberwachung und/oder Strafverfolgung durchführen, könnte EUROSUR außerdem auch von den Verteidigungskräften Daten erhalten.[148] Daher ist es mehr als unglücklich, dass der EUROSUR-Vorschlag keinerlei Hinweise auf den gemeinsamen Informationsraum enthält.

141 Ebd. S. 99.
142 KOM (2010) 584 endgültig, S. 7.
143 Schlussfolgerungen des Rates zur Integration der Meeresüberwachung, 23. Mai 2011, S. 2.
144 KOM (2010) 584 endgültig, S. 6.
145 Ebd. S. 6.
146 Ebd. S. 12.
147 Ebd.S. 3.
148 Zur Zusammenarbeit zwischen Akteuren der ESVP und zivilen Akteuren der Meeresüberwachung siehe: Europäische Verteidigungsagentur, Abschlussbericht des Wise Pen Team vom 26. April 2010, S. 23-27.

3.1.1.1 Notwendige Sicherheitsvorkehrungen

Der Verordnungsvorschlag der Kommission erwähnt den Datenschutz ausschließlich in der Präambel in Bezug auf den Austausch personenbezogener Daten mithilfe des EUROSUR-Kommunikationsnetzes und geht nicht einmal in diesem Zusammenhang auf die Erhebung personenbezogener Daten ein, die vermutlich im Rahmen von EUROSUR auf einigen Ebenen stattfinden wird.[149] Die FRONTEX-Verordnung (aktuelle Fassung) ist die *lex specialis* für die Tätigkeiten von FRONTEX in diesem Zusammenhang. In den Bereichen, in denen die FRONTEX-Verordnung keine „umfassende Datenschutzregelung" enthält, gelten die Datenschutzvorschriften der Richtlinie 95/46/EG, der Verordnung (EG) Nr. 45/2001 sowie - im Rahmen der polizeilichen und justiziellen Zusammenarbeit - der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008.

FRONTEX darf personenbezogene Daten verarbeiten, die von den Mitgliedstaaten im Rahmen von gemeinsamen Operationen, Pilotprojekten und Soforteinsätzen über Personen erfasst wurden, „die von den zuständigen Behörden der Mitgliedstaaten hinreichend begründet der Beteiligung an grenzüberschreitenden kriminellen Handlungen, der Beihilfe zur illegalen Einwanderung oder Aktivitäten in Bezug auf den Menschenhandel gemäß Artikel 1 Absatz 1 Buchstaben a und b der Richtlinie 2002/90/EG des Rates verdächtigt werden."[150] Diese Daten können für die Erstellung von Risikoanalysen verwendet, müssen aber im Ergebnis der Risikoanalyse anonymisiert werden.[151] Allerdings können diese Daten „nach Einzelfallentscheidung" an Europol oder „andere Strafverfolgungsbehörden der Union" übermittelt werden. Danach werden die Daten gelöscht. FRONTEX darf derartige Daten keinesfalls länger als drei Monate speichern.[152] Es ist unklar, wie die mögliche Überwachung bestimmter Häfen und Küsten in Drittländern durch Drohnen von FRONTEX mit dieser Vorschrift in Einklang gebracht werden soll, da Drohnen vermutlich die Daten über alle Personen verarbeiten können, die sich in diesen Bereichen aufhalten, d. h. auch von besonders gefährdeten Personen, die vor Verfolgung flüchten und besonderen Schutz benötigen. Wie die Frühjahrskonferenz der europäischen Datenschutzbeauftragten im Jahr 2008 feststellte, muss „die Überwachung von Reisenden begründet sein und ist nur in Ausnahmefällen und für rechtmäßige und spezielle Zwecke zulässig. Jede allgemeine Überwachung stellt eine unannehmbare Gefährdung der persönlichen Freiheit dar."[153]

Die EUROSUR-Verordnung sollte eine einschlägige Bestimmung enthalten, die ausdrücklich und vollständig die Bedingungen aufzählt, unter denen personenbezogene Daten im Rahmen von EUROSUR verarbeitet werden dürfen.[154] Außerdem müssen die Rechte der registrierten Personen, einschließlich des Rechts auf Einsicht in die erfassten Daten, weiter verdeutlicht werden. Es ist zwar ermutigend, dass der Vorschlag den Austausch von Informationen mit einem Drittland, das diese verwenden könnte, um Personen oder Gruppen ausfindig zu machen, die ernsthaft gefährdet sind, Opfer von Folter, einer unmenschlichen oder erniedrigenden Behandlung oder Strafe oder einer

149 Präambel 7, Verordnungsvorschlag.
150 Artikel 11.c.2 der FRONTEX-Verordnung.
151 Artikel 11.c.3 der FRONTEX-Verordnung.
152 Artikel 11.c.3 der FRONTEX-Verordnung.
153 Frühjahrskonferenz der europäischen Datenschutzbeauftragten, Rom 17.–18. April 2008.
154 Siehe auch die Anmerkungen des Europäischen Datenschutzbeauftragen zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Europäischen Grenzüberwachungssystems (EUROSUR) (KOM (2011)873 endgültig), vom 8. Feb. 2012, S. 1.

anderen Verletzung der Grundrechte zu werden, eindeutig untersagt,[155] allerdings bleibt unklar, wie diese Bestimmung in der Praxis durchgesetzt werden soll. Da der Datenaustausch durch EUROSUR mit „benachbarten Drittländern" auf der Grundlage bilateraler oder multilateraler Vereinbarungen zwischen einem oder mehreren Mitgliedstaaten und einem oder mehreren Drittländern erfolgen würde,[156] wäre es wünschenswert, eine Meldepflicht für diese Art von Datenaustausch einzuführen, damit die einzelstaatlichen Aufsichtsorgane die Weitergabe von Daten an Drittländer kontrollieren können. Die EUROSUR-Verordnung sollte außerdem ausdrücklich ein stufenweise aufgebautes Kontrollsystem vorsehen, bei dem die nationalen Datenschutzbeauftragten die Verarbeitung personenbezogener Daten durch die nationalen Koordinierungszentren überwachen und der europäische Datenschutzbeauftragte (EDPS) die Verarbeitung personenbezogener Daten durch FRONTEX kontrolliert.

3.1.2 „Intelligente Grenzen"

Obschon die Einzelheiten der Initiative „Intelligente Grenzen" nicht feststehen, lassen sich die datenschutzrechtlichen Probleme der beiden enthaltenen Systeme relativ klar erkennen. In diesem Bericht liegt der Schwerpunkt auf den datenschutzrechtlichen Bedenken zum Einreise-/Ausreisesystem (EES), da die Entwicklung des Registrierungsprogramms für Reisende (RTP) stark von der Entwicklung des EES abhängt.

Sowohl EES als auch RTP sehen die Schaffung einer zentralisierten europäischen Datenbank vor, die möglicherweise höchst sensible biometrische Daten, wie Fingerabdrücke und Gesichtsbilder enthält. Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte stellt bereits die bloße Speicherung von Daten eine Verletzung des Rechts auf Privatsphäre dar. Der Gerichtshof hat in der Beschwerdesache *S. und Marper gegen das Vereinigte Königreich* deutlich gemacht, dass Fingerabdrücke und Fotos einmalige Informationen enthalten, die „geeignet sind, das Privatleben zu beeinträchtigen." Daher kann nach Ansicht des Gerichtshofs die Speicherung dieser Informationen ohne Zustimmung der betroffenen Personen „nicht als neutral oder unbedeutend abgetan werden."[157]

Personen, die sich im RTP registrieren lassen möchten, müssten den Einwanderungsbehörden freiwillig Daten bereitstellen, die über die Informationen, die zum Erhalt eines Visums oder zur Registrierung als Staatsbürger eines Drittlands, für das keine Visapflicht besteht, hinausgehen.[158] Personen, die der Verarbeitung ihrer Daten im Rahmen dieser Sicherheitsüberprüfung zustimmen, müssen umfassend über die genauen Modalitäten für die Verarbeitung und Speicherung ihrer Daten informiert werden, damit ihre Zustimmung auf einer ausreichenden Informationsgrundlage beruht. Drittstaatenangehörige, die in die Union einreisen möchten, hätten keine andere Wahl, als der Verarbeitung ihrer personenbezogenen Daten zuzustimmen. Angesichts der Menge an Daten, die erfasst werden soll, müsste überzeugend nachgewiesen werden, dass dies zum Schutz der

155 Artikel 18.2, EUROSUR-Verordnungsvorschlag.
156 Artikel 18.1, EUROSUR-Verordnungsvorschlag.
157 Beschwerdesache S. und Marper gegen das Vereinigte Königreich, Bsw. 30562/04 und Bsw. 30566/04, Urteil vom 4. Dezember 2008, Absatz 84.
158 Siehe auch SEC (2008) 153 final, S. 57.

öffentlichen Sicherheit oder öffentlichen Ordnung erforderlich ist. In jedem Fall muss die Datenerfassung durch einen Rechtsrahmen reguliert werden, der ausreichende Sicherheitsvorkehrungen zum Schutz von Privatsphäre und personenbezogenen Daten vorsieht. Daher müssen als Mindestvoraussetzung die relevanten Sicherheitsvorschriften, die für ähnliche Datenbanken wie VIS, SIS und SIS II gelten, auch auf EES und RTP angewendet werden.

Entsprechend dem Urteil des Gerichtshofs der Europäischen Gemeinschaften in der Rechtssache *Huber* ließe sich argumentieren, dass eine zentralisierte Datenbank zur Unterstützung der mit der Anwendung aufenthaltsrechtlicher Vorschriften betrauten Behörden grundsätzlich legitim und angesichts ihrer Natur mit dem in Art. 18 Abs. 1 AEUV niedergelegten Verbot der Diskriminierung aus Gründen der Staatsangehörigkeit vereinbar ist. Allerdings darf ein solches Register keine anderen Informationen enthalten als die, die zu dem genannten Zweck erforderlich sind."[159] Derzeit ist der Zweck des EES nicht ausreichend deutlich bestimmt, weshalb diese Vorgabe nicht erfüllt ist.

Nach Artikel 7 Absatz e der Datenschutzrichtlinie ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie „erforderlich ist für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde." Nach Angaben der Kommission soll das EES „vor allem" zur Überwachung der „Einhaltung der zulässigen Aufenthaltsdauer von Drittstaatsangehörigen (...) als zentralem Bestandteil einer Risikobewertung an vorderster Front" dienen. Außerdem soll das System „zur Optimierung der Grenzkontrollverfahren und zur Verbesserung der Sicherheit durch diese beim Grenzübertritt an den Außengrenzen ansetzende Maßnahme beitragen."[160] Das EES ist also vor allem als Instrument zur Migrationskontrolle gedacht, das „die Zahl der erfolgreichen Rückführungen von sich irregulär im Schengen-Raum aufhaltenden Drittstaatsangehörigen erhöht."[161] Diese Argumentation weist jedoch einige Schwächen auf. Es gibt viele rechtmäßige Gründe für die Überziehung der genehmigten Aufenthaltsdauer und viele Ausnahmen im Schengener Grenzkodex bezüglich der Registrierung von Ein- und Ausreisen. Daher ist kaum anzunehmen, dass eine EES-Warnmeldung als einzige Begründung für eine Abschiebung oder Ausweisung ausreicht. Eine Warnmeldung kann daher nur eine *Vermutung* des illegalen Aufenthalts begründen.

Wenn eine Warnmeldung immer dann ausgelöst würde, wenn jemand seine genehmigte Aufenthaltsdauer überschreitet, würde das System auch Personen melden müssen, die dafür vollkommen rechtmäßige Gründe haben. Dies wäre beispielsweise der Fall, wenn die Betreffenden einen Asylantrag gestellt oder eine Verlängerung der Aufenthaltsgenehmigung erhalten haben, und daher nicht gemäß ihrer ursprünglichen Aufenthaltsbedingungen wieder ausgereist sind. „Überziehungen" können auch durch Umstände verursacht werden, für die der Betreffende nicht verantwortlich ist, beispielsweise eine schwere Erkrankung, einen Unfall, Flugausfälle usw. Nicht zuletzt können Warnmeldungen auch von Anomalien im System ausgelöst werden: ein Drittstaatangehöriger ist aus- und an einer Außengrenze wieder eingereist, an der keine Daten erfasst werden, das Besatzungsmitglied eines Flugzeugs reist als normaler Fahrgast ein usw.[162] Die

159 Rechtssache C-524/06, Heinz Huber gegen Bundesrepublik Deutschland.
160 KOM (2011) 680 endgültig, S. 5.
161 Ebd.. S. 12; siehe auch Dokument des Rates Nr. 16042/11, S. 27.
162 Siehe insbesondere die in Anhang VI und VII des Schengener Grenzkodex genannten Ausnahmen.

Grundsätze der Datenqualität[163] verlangen, dass alle angemessenen Maßnahmen zu treffen sind, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden. Es ist offen, ob ein EES mit den genannten Ausnahmen und Anforderungen umgehen kann.

Ein Einreise-/Ausreisesystem kann nur funktionieren, wenn es fehlerfrei jede Einreise und jede Ausreise sämtlicher Drittstaatenangehörigen erfasst. Wie aber bereits der Europäische Datenschutzbeauftragte aufgezeigt hat, kann sich nicht jeder Mensch in einem Programm registrieren, das biometrische Daten verwendet. Der Europäische Datenschutzbeauftragte nennt Krankheit, Behinderung, Wunden und Verbrennungen als mögliche Hinderungsgründe.

> „Das Phänomen kann gelegentlich auch mit der Volkszugehörigkeit oder dem Beruf zu tun haben. So hat insbesondere eine nicht unerhebliche Anzahl von Land- und Bauarbeitern Fingerkuppen, die so beschädigt sind, dass ihre Fingerabdrücke unlesbar sind. In anderen Fällen, deren Häufigkeit nur schwer zu bestimmen ist, kann es vorkommen, dass sich Flüchtlinge selbst verstümmeln, damit ihnen keine Fingerabdrücke abgenommen werden können.“ [164]

Angesichts der Fehleranfälligkeit von biometrischen Erfassungssystemen und der Möglichkeit von Systemunterbrechungen[165], sind „Rückfall”-Verfahren erforderlich, die auch Personen, die sich nicht registrieren konnten, die Einreise ermöglichen. Die Kommission behauptet, das EES halte Drittstaatenangehörige davon ab, ihre genehmigte Aufenthaltsdauer zu überziehen. Angesichts der vielen möglichen Schlupflöcher im System ist diese Aussage jedoch äußerst fragwürdig.

Außerdem ist es nach derzeitiger Rechtslage nicht möglich, eine EES-Warnmeldung in das SIS bzw. SIS II-System einzuspeisen, das nur die Aufnahme von Ausweisungsbescheiden eines Gerichts oder einer anderen zuständigen Behörde erlaubt. Ob sich eine Person rechtmäßig auf dem Gebiet der Europäischen Union aufhält, lässt sich nur in einem Verwaltungsverfahren bestimmen. Da also ein „Treffer“ im EES keine unmittelbaren Folgen für Überzieher/-innen hat, ist äußerst fraglich, ob das System wirklich zu effizienteren Rückführungen beiträgt. Jeder Versuch, EES-Warnmeldungen automatisch mit SIS bzw. SIS II zu verknüpfen, würde höchstwahrscheinlich zur Kontrolle von einer inakzeptabel großen Anzahl absolut legaler Reisender führen. Außerdem darf man nicht vergessen, dass die Grenzposten bereits überprüfen, ob ausreisende Visainhaber ihre genehmigte Aufenthaltsdauer überzogen haben. Die Einführung von halbautomatischen Kontrollen würde ihnen diese Aufgabe nicht abnehmen, sondern höchstens erleichtern.

Als weiteres Argument für das EES wird angeführt, es stelle eine großartige Quelle für statistische Daten über einschlägige Muster (z. B. Reiserouten, in betrügerischer Absicht ausgestellte Einladungen, Herkunftsland und Reisegründe) sowie für Daten über Migrationsströme und Overstayer für visumpolitische Zwecke dar.[166] Laut der Zusammenfassung der Ergebnisse der EU-

163 Siehe Artikel 6.1.(d) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

164 Stellungnahme des Europäischen Datenschutzbeauftragten zu „Eurodac“ 2011/C 101/03, S.4

165 Über das aktuelle Versagen einer biometrischen Datenbank berichtete die BBC im Artikel „UK Border Agency ID card system crashes“, 3. Mai 2012, unter://www.bbc.co.uk/news/uk-17943589

166 KOM (2008) 69 endgültig, S. 8.

Konferenz über innovatives Grenzmanagement durch die dänische Ratspräsidentschaft vertraten verschiedene Teilnehmer der Konferenz die Auffassung, dass das EES als „Instrument“ zur Aufdeckung, Identifizierung und Ermittlung der Zahl der Personen, die nach Ablauf ihrer Aufenthaltsgenehmigung im Land bleiben, dienen könne, „welches nützliche Informationen zur Debatte über illegale Einwanderung und zur Unterstützung des Vorgehens gegen die Schwarzmarktwirtschaft beisteuern und sich auch im Hinblick auf das Verhältnis zu Drittländern, z. B. betreffend die Visumpolitik, als nützlich erweisen könne.“ [167] Die Speicherung und Verarbeitung von Unmengen personenbezogener Daten in einer derartigen Datenbank dürfte kaum erforderlich sein im Sinne von Artikel 7 Absatz e der Richtlinie 95/46. Der Europäische Gerichtshof hat sich in der Rechtssache Huber äußerst klar geäußert:

> „Zwar hat das Gemeinschaftsrecht den Mitgliedstaaten nicht die Befugnis zum Erlass von Maßnahmen genommen, die den nationalen Behörden die genaue Kenntnis der Bevölkerungsbewegungen in ihrem Hoheitsgebiet ermöglichen sollen, doch macht die Ausübung dieser Befugnis die Erhebung und Aufbewahrung von namentlich genannte Personen betreffenden Daten nicht erforderlich. Dieses Ziel erfordert nämlich nur die Verarbeitung anonymer Informationen.”[168]

Im politischen Prozess wurden zahlreiche weitere Begründungen für die Schaffung eines EES genannt, beispielsweise dass das System Bedrohungen gegen die innere Sicherheit der Mitgliedstaaten verhindern könne, insbesondere durch die Verhinderung, Erfassung und Untersuchung von terroristischen Anschlägen und Verbrechen der organisierten Kriminalität. Dies könnte dazu führen, dass zahlreiche weitere Daten über Drittstaatangehörige ohne Visapflicht im EES erfasst werden, die den durch das Visa-Informationssystem erfassten Daten ähneln, beispielsweise Angaben zu Mitreisenden (wenn eine Person als Teil einer Gruppe reist), Anschrift des Beherbergungsbetriebs oder des Wohnorts, Hauptreiseziel und Zweck der Reise oder des Aufenthalts.[169] Einige Mitgliedstaaten haben vorgeschlagen, Angaben über die Fahrzeuge aufzunehmen, die Drittstaatenangehörige für die Einreise in den Schengenraum über eine Landgrenze verwenden, und bestimmte Gegenstände zu melden, die diese bei sich tragen (z. B. Waffen oder Banknoten). Werden diese Vorschläge umgesetzt, besteht die Gefahr, dass die Polizei und andere Strafverfolgungsbehörden, Einwanderungsbehörden, das Außenministerium, Behörden, die für die Verhinderung, Erfassung und Verfolgung von terroristischen Verbrechen und anderen schweren Straftaten zuständig sind, oder deren Entsprechungen auf regionaler oder kommunaler Ebene Zugriff auf das EES erhalten. Dies wäre aus datenschutzrechtlichen Gründen äußerst bedenklich.

Entgegen den ursprünglichen Behauptungen von Kommissar Frattini hat die Kommission bereits selbst zugegeben, dass „das Potenzial (eines EES) zur Eindämmung von Terrorismus und von Schwerkriminalität nicht signifikant erscheint.”.[170] Die Kommission stellt fest, dass „die Mehrheit der

167 Dokument des Rates 7166/12 vom 2. März 2012, S. 6. Außerdem „können mit dem EES zuverlässige Daten gewonnen werden, die andernfalls fehlen würden, da mehr Drittländer eine Visaliberalisierung gewährt werde.“

168 Rechtssache Huber, Leitsatz 2

169 Siehe Artikel 9, VIS Verordnung.

170 SEC (2008) 154 final.

Personen, denen die Einreise verweigert wird, weder Terroristen noch Schwerkriminelle sind, sondern Menschen ohne ordnungsgemäße Reisepapiere, die als mögliche illegale Zuwanderer verdächtigt werden.“.[171] Theoretisch könnte das EES Daten über die Reisen von Drittstaatenangehörigen erfassen, die keiner Visapflicht unterliegen, insbesondere, wenn diese als „verdächtig“ gelten. Nach Angaben der Kommission „könnten derartige Daten über die Bewegungen von Personen, die verdächtigt werden, Terroristen oder Schwerkriminellen zu sein, dazu dienen, deren Aufenthalt zu bestimmen und strafrechtlich zu verfolgen.“ Wie der Bericht von Steve Peers feststellt, „wenn eine Person, die in den Schengenraum eingereist ist, später einer terroristischen Aktivität verdächtigt wird, besteht mit Hilfe des Einreise-/Ausreisesystems die eingeschränkte Möglichkeit festzustellen, ob (und gegebenenfalls wann und wo) der Verdächtigte den Schengenraum verlassen hat, sofern der Verdächtigte auf legalem Weg aus dem Schengenraum ausreist.“ [172]Dies ist die wichtigste Begründung für die langfristige Speicherung von Daten zu Personen, die den Schengenraum auf absolut legalem Weg verlassen haben. Die Speicherung dieser Daten lässt sich jedoch kaum mit dem ursprünglichen Zweck vereinbaren, zu dem die Daten erfasst wurden.

Die Schaffung des EES wird ferner damit gerechtfertigt, das System könne eingesetzt werden, um Missbrauch im Bereich der Arbeitsmigration und insbesondere Kurzaufenthalte zu Arbeitszwecken zu verhindern. In diesem Fall könnten auch staatliche Behörden im Bereich Beschäftigung und Sozialversicherung Zugriff auf das EES erhalten. Auch als Mittel im Kampf gegen Korruption wird das EES genannt, da Daten, die durch das EES gewonnen werden, zur Identifizierung von Grenzschützer/-innen an bestimmten Grenzübergängen verwendet werden können. Auf diese Weise könnte beispielsweise untersucht werden, warum an bestimmten Grenzübergängen ungewöhnlich viele gefälschte Pässe nicht erkannt werden.

3.1.2.1 Notwendige Sicherheitsvorkehrungen

Obwohl nach Ansicht der Verfasser die Notwendigkeit des EES nicht überzeugend nachgewiesen werden konnte, möchten wir auf einige Sicherheitsvorkehrungen hinweisen, die ein möglicher Legislativvorschlag enthalten muss. Da das EES vor allem ein Instrument zur Zuwanderungskontrolle darstellt, wäre ein routinemäßiger Zugriff von Strafverfolgungsbehörden (oder Behörden im Bereich Beschäftigung und Sozialversicherung) auf die Daten des EES rechtswidrig. Erstens muss der Zugriff von Sicherheitsorganen auf Datenbanken, in denen „unschuldige“ Personen erfasst sind, viel stärker eingeschränkt sein, als der Zugriff auf Verbrecherdatenbanken. Zweitens würde ein derartiger Routinezugriff bedeuten, dass ein unleugbarer Zusammenhang zwischen dem organisierten Verbrechen und Drittstaatenangehörigen, einschließlich Asylsuchenden und illegalen Einwanderern, besteht. Wie ein Beobachter festgestellt hat: „da ein derartiger Zusammenhang nicht nachgewiesen wurde und ähnliche Maßnahmen, wie z. B die zentrale Speicherung von sensiblen

171 SEC (2008) 153 final, p. 9.
172 Peers, “Proposed new border control systems”, S. 9.

personenbezogenen Daten aller EU-Bürger fehlen, ist zu fragen, ob die Weiterverfolgung nicht sogar eine Diskriminierung darstellt."[173]

Die Notwendigkeit des Zugriffs muss in jedem Einzelfall nachgewiesen werden und zeigen, dass die Daten nicht, oder nur unter großen Schwierigkeiten, auf anderem Wege erhältlich sind, die keinen derartigen starken Eingriff bedeuten. Um eine Überprüfung dieses Grundsatzes zu ermöglichen, könnte ein Protokoll eingeführt werden, das jeden Zugriff von Strafverfolgungsbehörden auf Daten des EES verzeichnet. Es muss ausdrücklich und restriktiv festgelegt werden, wann die Verwendung der Daten rechtmäßig ist, und die Festlegung muss über allgemeine Aussagen wie „für die Erfüllung ihrer Aufgaben erforderlich" hinausgehen.

Das Auskunftsrecht der Personen, die sich im RTP registrieren lassen möchten und der Drittstaatenangehörigen, die in die Union einreisen und deren Daten im EES verarbeitet werden, muss durch wirksame Datenschutzregelungen geschützt sein. Sie müssen über die Identität der für die Verarbeitung Verantwortlichen, die Zwecke der Datenverarbeitung, die Kategorien der Datenempfänger, die Aufbewahrungsfrist der Daten und ihr Auskunftsrecht bezüglich der über sie gespeicherten Daten informiert werden. Außerdem müssen sie darüber informiert werden, dass sie die Löschung von Daten verlangen können, die unrichtig sind oder unrechtmäßig verarbeitet wurden, sowie über die Verfahren zur Ausübung dieser Rechte und die einzelstaatlichen Kontrollbehörden, die Beschwerden hinsichtlich des Schutzes personenbezogener Daten entgegennehmen.[174]

Die Betroffenen haben ein Recht, die Beschwerdeverfahren zu kennen, mit denen sie gegen eine Ablehnung ihrer Registrierung im RTP oder eine Einstufung als Overstayer Beschwerde einlegen können. Außerdem muss eine Möglichkeit geschaffen werden, gegen diese Entscheidungen Beschwerde einzulegen oder deren Überprüfung durch zuständige Gerichte oder Behörden zu erreichen, deren Mitglieder unparteiisch und in den Mitgliedstaaten, die „Überziehungswarnmeldungen" ausgeben, unabhängig sind und die Angemessenheit und Rechtmäßigkeit der Maßnahme beurteilen.[175] Artikel 22 der Datenschutzrichtlinie der EU legt eindeutig fest, dass „jede Person" ungeachtet ihres Wohnorts einen Rechtsbehelf einlegen kann, d. h. auch Drittstaatenangehörige.

Wie obenstehend erläutert, sind strenge Datenschutzbestimmungen unerlässlich, da die im EES gespeicherten Daten für zahlreiche Zwecke verwendet werden könnten, die die Interessen der betroffenen Personen verletzten. Die Europäische Kommission hat zugegeben, dass dies „wie bei

173 Audelina Ahumada, „Border control and internal security in the European Union – information, technology and human rights implications for third-country nationals", Detecter Deliverable 14(1) (Dez. 2008): S. 19, erhältlich unter: http://www.detecter.bham.ac.uk/D14.1BorderControlInternalSecurity-2.doc.

174 Siehe die entsprechenden Artikel 37–38 der VIS-Verordnung.

175 SEC (2008) 153 final, S. 58. Siehe auch Artikel 40 der VIS-Verordnung. Siehe auch Seite 2 der entsprechenden Empfehlung des Meijers Ausschusses zu Artikel 43 der geänderten SIS-II-Verordnung: „2. Alle Personen haben das Recht, bei den gemäß dem Recht der Mitgliedstaaten zuständigen Gerichten oder Behörden Rechtsbehelf einzulegen, um die Einsicht in und die Richtigstellung oder Löschung von Daten oder Schadenersatz für eine Warnmeldung bezüglich der eigenen Person zu erlangen. 3. Die Mitgliedstaaten verpflichten sich, die rechtskräftigen Entscheidungen der im Abschnitt 1 und 2 genannten Gerichte und Behörden ungeachtet der Bestimmungen in Artikel 48.4. zu vollstrecken. Die Regelungen der in diesem Artikel regulierten Rechtsbehelfe werden durch die Kommission überprüft […]."

allen Daten dieser Art, die unrechtmäßig verwendet werden können, ein mögliches Problem“ darstellt.”[176] Es müssen gesetzliche Bestimmungen eingeführt werden, die auch Drittstaatenangehörigen, die sich nicht in einem System, das biometrische Daten verwendet, anmelden konnten, die Einreise ermöglicht.[177]

3.2 Auswirkungen auf das Recht auf Asyl

Sowohl das EES als auch EUROSUR können die Rechte von Flüchtlingen und Menschen, die einen Asylantrag stellen möchten, beeinträchtigen. Der Europäische Datenschutzbeauftragte hat diese mittelbare Auswirkung von Grenzschutzmaßnahmen betont und festgestellt, dass sie „Menschen davon abhalten können, in Europa den Schutz zu suchen, auf den sie gemäß dem internationalen Recht zum Schutz von Flüchtlingen ein Anrecht haben.“[178] Tatsächlich ist die Forderung nach Schaffung von EUROSUR und "intelligenten Grenzen" Teil einer langfristigen Entwicklung, die es Flüchtlingen und anderen schutzbedürftigen Personen immer mehr erschwert, in die Europäische Union zu gelangen. Beide Systeme dienen eindeutig dem Zweck, die Grenzüberwachung der EU über die tatsächlichen Grenzen der Union hinaus auf die hohe See und das Staatsgebiet von Drittländern (in den „Grenzvorbereich“) auszudehnen. Diese Entwicklung lässt sich nur als gemeinsame Anstrengung der Mitgliedstaaten deuten, die Verantwortung für Asylansprüche zu vermeiden. Obwohl die Systeme die rechtlichen Verpflichtungen der Mitgliedstaaten nach Artikel 18 der EU-Grundrechtcharta und des Genfer Abkommens über die Rechtsstellung von Flüchtlingen nicht berühren,[179] sind spezielle Sicherheitsvorkehrungen notwendig, die gewährleisten, dass Flüchtlinge, die in Europa Asyl beantragen möchten, dies auch tun können.

3.2.1 EUROSUR

EUROSUR wirkt sich sowohl positiv als auch negativ auf das Recht auf Asyl aus. Der Vorschlag der Kommission sieht vor, dass die Mitgliedstaaten und die Agentur Frontex bei der Anwendung der EUROSUR-Verordnung „den besonderen Bedürfnissen von Kindern, Opfern des Menschenhandels, Personen, die dringend medizinische Versorgung oder internationalen Schutz benötigen, Personen in Seenot und anderen Personen, die sich in einer besonders schwierigen Situation befinden“, Vorrang einräumen.[180] In früheren Mitteilungen hat die Kommission wiederholt betont, einer der wichtigsten Gründe für die Schaffung von EUROSUR sei die Rettung von Personen, die sich in Seenot befinden. Wenn kleine, überfüllte und nicht seetüchtige Boote ohne Rettungsausstattung oder Beleuchtung

176 SEC (2008) 153 final, S. 57.

177 Europäischer Datenschutzbeauftragter, Stellungnahme zum VIS, ABl. C 181/19.

178 Preliminary Comments of the EDPS 2008, S.6

179 Wie Präambel 16 des EUROSUR-Verordnungsvorschlags ausdrücklich feststellt, lässt „die Durchführung dieser Verordnung (…) die Verpflichtungen der Mitgliedstaaten aus dem Seerechtsübereinkommen der Vereinten Nationen, dem Internationalen Übereinkommen zum Schutz des menschlichen Lebens auf See, dem Internationalen Übereinkommen über den Such- und Rettungsdienst auf See, dem Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität und dem dazugehörigen Zusatzprotokoll gegen die Schleusung von Migrant/-innen auf dem Land-, Luft- und Seeweg, dem Abkommen über die Rechtsstellung der Flüchtlinge, der Konvention zum Schutze der Menschenrechte und Grundfreiheiten und anderen einschlägigen internationalen Übereinkünften unberührt.“ Der EES-Verordnungsvorschlag muss eine entsprechende Bestimmung enthalten.

180 Artikel 2.3, EUROSUR-Verordnungsvorschlag.

frühzeitig entdeckt würden, könnten die Agentur Frontex oder ein Mitgliedstaat einen Rettungseinsatz einleiten und Menschenleben retten.[181]

Es wird behauptet, EUROSUR unterstütze die Such- und Rettungskräfte der Mitgliedstaaten und gewährleiste, „dass so viele Menschen wie möglich in Sicherheit gebracht werden."[182] Die Unterstützung der Such- und Rettungseinsätze „berühren nicht Funktion und Aufgabe der zuständigen SAR-Leitstellen."[183] Auch die Agentur der Europäischen Union für Grundrechte (FRA) ist der Meinung, „das lebensrettende Potenzial des EUROSUR-Systems sollte optimal genutzt werden", weil es frühzeitig Informationen über Schiffe oder Personen bereitstellen kann, die sich in schwerer und unmittelbarer Gefahr befinden und sofortige Hilfe benötigen.[184] Obwohl wir die Meinung der Agentur für Grundrechte teilen, befürchten wir, dass dieses Potenzial ungenutzt bleibt, wenn die Priorität von Such- und Rettungseinsätzen nicht ausdrücklich festgelegt wird. EUROSUR könnte eindeutig dazu beitragen, mehr Menschen „in Sicherheit" zu bringen. Aber der Vorschlag erläutert an keiner Stelle, wie genau dies erreicht werden soll und ebenso wenig, wie weiter mit den „Geretteten" verfahren wird. In den betreffenden Booten befinden sich meistens irreguläre Migrant/-innen und Menschen, die den Schutz der internationalen Gemeinschaft benötigen, aber dass Letztere einen Asylantrag stellen müssen, wird nicht erwähnt. Im Gegenteil stellt Artikel 2.2. des Verordnungsentwurfs fest, dass die EUROSUR-Verordnung „nicht für operative, verfahrenstechnische und rechtliche Maßnahmen gilt, die nach Abfang- beziehungsweise Aufgriffsmaßnahmen getroffen werden." Die Folgenabschätzung formuliert noch eindeutiger: „Asyl, Rückübernahme und Rückkehr" liegen außerhalb des Zuständigkeitsbereichs von EUROSUR.[185]

Wenn die EU ehrlich an der Rettung von Menschen aus Seenot interessiert ist, muss sie zumindest festlegen, wie EUROSUR Informationen oder Warnmeldungen an die Rettungsleitstelle des für das Such- und Rettungsgebiet zuständigen Landes übermittelt. In diesem Zusammenhang ist zu beachten, dass die Ergänzung des Schengener Grenzkodex aus dem Jahr 2010 bereits im nicht verbindlichen Anhang über „Leitlinien für Such- und Rettungsmaßnahmen und für die Ausschiffung im Rahmen von durch die Agentur koordinierten Maßnahmen an den Seegrenzen" eine entsprechende Bestimmung enthält.[186] Insbesondere angesichts des aktuellen „Hirsi"-Urteils, in dem die Gesetzwidrigkeit italienischer Rückführungsaktionen nach Libyen festgestellt wurde, muss hier ein grundsätzliches Argument angeführt werden.[187] Staaten können Flüchtlingsrecht und Menschrechte nicht einfach umgehen, indem sie Abfangeinsätze auf hoher See, mit denen Migrant/-innen am Erreichen der EU-Grenzen gehindert werden, mit Such- und Rettungseinsätzen gleichstellen, wie dies in den derzeit geltenden Richtlinien für gemeinsame Einsätze der Fall ist. Ohne strenge Richtlinien für die Agentur Frontex und die Mitgliedstaaten wird in der Praxis mit größter

181 Siehe auch (SEC (2011) 1536 final, S. 9, und die Parlamentarische Anfrage, E-006760/2011; Antwort von Frau Malmström für die Kommission (28. Juli 2011).

182 Ebd.

183 SEC (2011) 1536 final, S. 14.

184 Agentur der Europäischen Union für Grundrechte, The Stockholm Programme: A chance to put fundamental rights protection right in the centre of the European Agenda, Wien, 14. Juni 2009, S. 8.

185 SEC (2011) 1538 final, S. 24.

186 Artikel 1.2 dieses Anhangs legt ausdrücklich fest: „wenn im Verlauf des Grenzüberwachungseinsatzes Zweifel an der Sicherheit eines Schiffes oder von Personen an Bord bestehen, übermitteln die beteiligten Einsatzkräfte der für die Such- und Rettungszone zuständigen Rettungsleitstelle so schnell wie möglich alle vorhandenen Lageinformationen."

187 Hirsi und andere gegen Italien, Bsw. 27765/09.

Sicherheit das Abfangen und die Zurückweisung von Flüchtlingen Vorrang vor deren Rettung und Schutz haben.

Die Technische Studie illustriert dieses Dilemma anhand von beispielhaften „operativen Informationen“, die EUROSUR im gemeinsamen Informationsbild des Grenzvorbereichs bereitstellt:

> 5. Mai 20XY: Gemäß den von XY bereitgestellten Satellitenbildern legten heute Morgen gegen 5.00 Uhr 7 Holzboote (Länge 12-15 m) mit rund 250 illegalen Migranten in der Nähe des Dorfes K (Koordinaten xy Ost yw West) bei schwierigen Witterungsbedingungen (Windstärke 5, zunehmend) von der Küste des afrikanischen Landes Z ab. Die Durchschnittsgeschwindigkeit des verwendeten Bootstyps beträgt 7-8 Knoten. Aufgrund der derzeitigen Einwanderungstrends ist zu erwarten, dass die Boote in Richtung MS A (Wahrscheinlichkeit 70 %) oder MS B (Wahrscheinlichkeit 30 %) unterwegs sind. Das Nationale Koordinierungszentrum A hat die Behörden von Land Z informiert, die trotz der vor Kurzem erhaltenen Patrouillenboote vermutlich nichts unternehmen werden. Das Nationale Koordnierungszentrum A koordiniert derzeit mit dem Nationalen Koordinierungszentrum B und FRONTEX (gemeinsamer Einsatz Karies) ihre Patrouilleneinsätze zur Suche und Rettung (SAR) und zum Abfangen. FRONTEX leitet aktuell Satelliten und zwei Überwachungsflugzeuge in den Bereich TOMATO (Route zum MS A) um. [188]

Trotz der „schwierigen Witterungsbedingungen" und der vermutlich überfüllten Boote ist das Ziel der Meldung und der anschließenden Überwachungsmaßnahmen im Beispiel nicht eindeutig vor allem die Rettung von Menschenleben, obwohl die Inhaber derartiger Informationen gemäß dem SOLAS-Übereinkommen verpflichtet sind, vorrangig jegliche mögliche Hilfe zu leisten. Derzeit enthält der EUROSUR-Verordnungsvorschlag keine Einzelheiten über das Ziel der „Rettung von Menschenleben auf See“, wogegen die Grenzüberwachungsfunktionen des Systems ausführlich dargestellt werden. Daher muss der Vorschlag unbedingt so ergänzt werden, dass die Verpflichtung zu Such- und Rettungsaktionen gestärkt wird und den Anforderungen des Flüchtlingsrechts und der allgemeinen Menschenrechte entspricht.[189] Die vermutliche Aufhebung der obengenannten Richtlinien für gemeinsame Einsätze eröffnet dem Europäischen Parlament die Möglichkeit, eine kohärente Politik zu fordern, die sich in Strategie und Praxis niederschlägt.

3.2.2 Einreise-/Ausreisesystem (EES)

Wie bereits ausgeführt, gibt es rechtmäßige Gründe, aus denen ein „Drittausländer“ seine genehmigte Aufenthaltsdauer überzieht, und Fälle, in denen das System Personen irrtümlich als Overstayer identifiziert. Daher müssen in das EES entsprechende Sicherheitsvorkehrungen integriert werden. Dies wäre beispielsweise der Fall, wenn der/die Betreffende einen Asylantrag gestellt oder eine Verlängerung der Aufenthaltsgenehmigung erhalten hat, und daher nicht gemäß den ursprünglichen Aufenthaltsbedingungen wieder ausgereist ist. Daher muss jede Rechtsvorschrift

188 Teilprojekt 3, Abschlussbericht – Gemeinsames Informationsbild des Grenzvorbereichs, „Technical and management concepts for the surveillance of land and maritime borders“, Technische Studie für die Generaldirektion für Justiz, Freiheit und Sicherheit der Europäischen Kommission, im Rahmen des Europäischen Grenzkontrollsystems (EUROSUR), Januar 2010, S. 26.

189 Violeta Moreno-Lax, „Seeking asylum in the Mediterranean: Against a fragmentary reading of EU Member States’ obligations accruing at sea“, International Journal of Refugee Law 23(2) (2011), S. 199. „Die Mitgliedstaaten und FRONTEX können das Abfangen von Migrant/-innen nicht zum Schutz von Menschenleben einsetzen, ohne zu bedenken, dass die Ausschiffung in Staaten vermieden werden muss, in denen Leben und Freiheit der Personen, die begründete Angst vor Verfolgung äußern oder denen tatsächliche Misshandlungen drohen, in Gefahr sind.“

über das EES unbedingt die Bestimmung enthalten, dass jede „Überziehungswarnmeldung“ nur die Vermutung eines unerlaubten Aufenthalts darstellt. Nach Ausgabe der Warnmeldung, lässt sich nur in einem Verwaltungsverfahren bestimmen, ob sich die betreffende Person rechtmäßig auf dem Gebiet der Europäischen Union aufhält. Dieses Verfahren muss dem Reisenden die Möglichkeit geben, die Umstände der „Überziehung“ zu erklären. Eine EES-Warnmeldung allein kann niemals als Begründung für die Einreiseverweigerung oder Ausweisung von Personen dienen und sollte daher nicht in das Schengener Informationssystem integriert werden.[190]Es ist tatsächlich nicht klar, wie irgendeine automatische Sanktion an eine EES-Warnmeldung geknüpft sein könnte. Geltungsbereich und Funktion des EES muss daher auf die Grenzschützer/-innen beschränkt sein, die Reisende kontrollieren, und Daten dürfen nur dann nach der Ausreise der registrierten Person aus der EU gespeichert werden, wenn die Vermutung eines illegalen Aufenthalts sich bestätigt hat.

190 Die Rückführungsrichtlinie 2008/115/EG sieht Sanktionen für den illegalen Aufenthalt oder die Überziehung der genehmigten Aufenthaltsfrist vor, zu denen Rückführungsbescheide (mit einer Frist zur freiwilligen Ausreise und einem Wiedereinreiseverbot) und Zwangsmaßnahmen zur Abschiebung von Drittstaatsangehörigen gehören.

4 Kosten, Erforderlichkeit und Wirksamkeit

Die Kosten für das EUROSUR-System im Zeitraum 2011-2020 werden auf 340 Mio. € geschätzt. Die Europäische Kommission hat weitere 1,1 Mrd. Euro aus dem geplanten Fonds für innere Sicherheit (ISF) 2014-2020 zur Finanzierung der Initiative „Intelligente Grenzen“ (Einreise-/Ausreisesystem und Registrierungsprogramm für Reisende) eingeplant. Dieser Bericht kann keine umfassende Folgenabschätzung des EUROSUR-Vorschlags und der geplanten Programme EES und RTP leisten. Stattdessen enthält er einige Anmerkungen zu den Machbarkeitsstudien und Kostenvoranschlägen, die für den politischen Entscheidungsprozess auf EU-Ebene erstellt wurden. Außerdem analysiert der Bericht die Forschungs- und Entwicklungsprojekte zugunsten der drei Systeme, die aus Mitteln des 53,2 Mrd. Euro schweren Siebten Rahmenprogramms (RP7 2007-2013) gefördert werden, und zeigt auf, wie auch der Außengrenzenfonds, das Finanzierungsinstrument für die Entwicklungszusammenarbeit und der ISF verwendet wurden oder werden, um die Einführung von EUROSUR, EES und RTP in den Mitgliedstaaten und in Drittstaaten zu finanzieren. Abschließend empfehlen wir der Europäischen Kommission, vor dem Hintergrund der Erfahrungen, die die Vereinigten Staaten bei dem Versuch gemacht haben, ähnliche Systeme zu entwickeln und einzuführen, ihre Vorschläge nochmals neu zu bewerten.

4.1 Machbarkeitsstudien und Kostenvoranschläge

Da die Legislativvorschläge zu EUROSUR, EES und RTP sich möglicherweise negativ auf die Grundrechte auf Schutz der Privatsphäre und Datenschutz auswirken, sollten diese Vorschläge einer „Erforderlichkeitsprüfung“ unterzogen werden. Laut einem Urteil des Europäischen Gerichtshofs für Menschenrechte ist ein Eingriff in die Grundrechte „erforderlich“, wenn er durch eine dringende soziale Notwendigkeit gerechtfertigt und dem verfolgten Ziel angemessen ist und die Gründe, die die Behörden zu seiner Rechtfertigung anführen, angemessen und ausreichend sind.[191] Insbesondere bei neuen Datenverarbeitungssystemen muss „ein klarer Beweis ihrer Notwendigkeit und Verhältnismäßigkeit” vorliegen, der durch eine sich auf „ausreichendes Beweismaterial” stützende Datenschutz-Folgenabschätzung erbracht werden” sollte.[192] Wie die Europäische Kommission selbst

191 Handyside gegen Vereinigtes Königreich, (Bsw. Nr. 5493/72), 7. Dez. 1976, § 48. Der Begriff der Erforderlichkeit bedeutet, dass mehr als nur die „Nützlichkeit“ bewiesen werden muss. Der Europäische Gerichtshof für Menschenrechte hat bei mehreren Gelegenheiten betont, dass das Adjektiv „erforderlich“ zwar nicht gleichbedeutend ist mit „unerlässlich“, jedoch auch nicht so flexibel wie die Begriffe „zulässig“, „üblich“, „nützlich“, „angemessen“ oder „wünschenswert“.

192 Stellungnahmen des Europäischen Datenschutzbeauftragten, 2012/C 34/02. Dies kann entweder durch eine spezielle Datenschutz-Folgenabschätzung erfolgen oder in die allgemeine Folgenabschätzung integriert werden. Die aktuellen Leitlinien zur Erstellung von Folgenabschätzungen (European Commission Impact Assessment Guidelines, SEC (2009) 92) sieht keine gesonderte Folgenabschätzung zu den Auswirkungen auf die Grundrechte, wie z. B. das Recht auf Datenschutz, vor. Stattdessen sollen diese Aspekte in der allgemeinen Folgenabschätzung berücksichtigt werden. Inzwischen wurde gemäß der Mitteilung der Kommission über eine Strategie zur wirksamen Umsetzung der Charta der Grundrechte durch die Europäische Union (KOM 2010/0573) als weiteres Hilfsmittel ein Arbeitsdokument der Kommissionsdienststellen über operative Leitlinien zur Berücksichtigung der Grundrechte in Folgenabschätzungen der Kommission (SEK (2011) 567 endgültig) erstellt.

zugibt, wäre „Nützlichkeit allein (…) also kein hinreichendes Kriterium für die Einführung eines Einreise-/Ausreisesystems oder eines Registrierungsprogramms für Reisende.“[193] Dennoch kritisiert der Europäische Datenschutzbeauftragte, dass in den allgemeinen Hinweisen der Europäischen Kommission nicht „konkrete Maßnahmen und Mechanismen bereitgestellt werden, mit denen gewährleistet wird, dass sowohl der Notwendigkeit als auch der Verhältnismäßigkeit Rechnung getragen wird und diese beiden Grundsätze in sämtlichen Vorschlägen mit Auswirkungen auf die Rechte des Einzelnen praktisch umgesetzt werden.“[194] Für EUROSUR wurde keine aussagekräftige Grundrechts- oder Datenschutz-Folgenabschätzung durchgeführt. Begründet wurde dies damit, dass das System nicht routinemäßig personenbezogene Daten verarbeitet, obwohl die Folgenabschätzung die Notwendigkeit einer gerechten und rechtmäßigen Verarbeitung zu klaren und rechtmäßigen Zwecken einräumt.[195] Bezüglich des EES konnte die Europäische Kommission noch nicht darlegen, dass die „wesentlichen Menschenrechtsverletzungen“, die in der Folgenabschätzung von 2004 festgestellt wurden, beseitigt werden konnten.[196]

4.1.1 EUROSUR

Vor Veröffentlichung des EUROSUR-Verordnungsvorschlags im Dezember 2011 wurden zahlreiche Studien und Folgenabschätzungen erstellt. Die BORTEC-Studie, eine Machbarkeitsstudie der Agentur FRONTEX, wurde 2007 fertig gestellt. 2008 legte die Europäische Kommission dann einen Fahrplan zur Einführung des EUROSUR-Systems und eine entsprechende Folgenabschätzung vor. Außerdem erstellte ein externes Forschungsinstitut im Jahr 2010 für 1,8 Mio. Euro eine weitere technische Studie, in denen die Verwaltungsverfahren für EUROSUR und die betrieblichen Anforderungen an das Kommunikationssystem und das gemeinsame Informationsbild zum Grenzvorbereich analysiert wurden. Im Jahr 2011 erstellte die Kommission eine zweite Folgenabschätzung, die gemeinsam mit dem Legislativvorschlag vorgelegt wurde. Als Beitrag zur zweiten Folgenabschätzung wurde eine Finanzuntersuchung zu EUROSUR in Auftrag gegeben. Die Autoren befürchten, dass durch dieses Verfahren keine angemessene demokratische Kontrolle und unparteiische Bewertung des EUROSUR-Vorschlags möglich war.

Machbarkeitsstudien sollen die Stärken und Schwächen einer bestimmten Vorgehensweise, deren mögliche Risiken und letztlich deren Erfolgschancen objektiv und rational untersuchen. Die BORTEC-Studie, die den Auftrag hatte, einen allgemeinen Rahmen für EUROSUR festzulegen, erfüllt als Machbarkeitsstudie nicht diese grundlegenden Anforderungen. Später nahm die Entscheidung, im Jahr 2008 mit der Entwicklung des Systems zu beginnen, die Ergebnisse aller künftigen Folgenabschätzungen vorweg. Wie die Kommission in ihrer Folgenabschätzung von 2011 feststellt: „Die Folgenabschätzung, die 2008 vorgestellt wurde, bewertete die verschiedenen Elemente, die in den Stufen 1 bis 7 des EUROSUR-Fahrplans vorgeschlagen wurden, und legte damit fest was zu tun ist. Die aktuelle Folgenabschätzung bewertet, wie diese Elemente auf der Grundlage der von 2008

193 KOM (2011) 680 endgültig, S. 13.

194 Stellungnahme des EDSB zur Mitteilung der Kommission „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht“, 2010/C 355/03, Absatz 28.

195 SEC (2011) 1536 final, S. 32.

196 European Policy Evaluation Consortium, „Study for the extended impact assessment of Visa Information System“, Dezember 2004, S. 31–37.

bis 2011 durchgeführten Maßnahmen bis 2013 umgesetzt werden sollen."[197] Das heißt, die Folgenabschätzung von 2008 begründete die Entscheidung für die Einführung von EUROSUR mit der Notwendigkeit, die Grenzen wirksamer zu kontrollieren (grundsätzlich war dies eine Entscheidung zwischen totaler Grenzkontrolle, einer technisch hochstehenden/intelligenten Grenzkontrolle und keiner Grenzkontrolle). Die Folgenabschätzung von 2001 bot dagegen nur drei politische Optionen und Kostenvoranschläge für die Einführung des Systems an. Die große Anzahl von Migrant/-innen und Flüchtlingen, die auf dem Weg nach Europa im Mittelmeer zu Tode kommen[198], ist bereits Grund genug für die Einrichtung eines Systems, mit dessen Hilfe Personen in Seenot gerettet werden können. Da jedoch keine detaillierten Richtlinien vorliegen, die festlegen, wie EUROSUR konkret Leben retten soll (von der Identifizierung gefährdeter Personen einmal abgesehen) lässt sich das lebensrettende Potential des Systems nur schwer abschätzen.

Außerdem ist zu befürchten, dass die Chancen, dass EUROSUR sein wichtigstes operatives Ziel erreicht (die ständige Überwachung der Hochsee zur Erkennung und Verfolgung kleiner Schiffe ab der Stelle, an der sie die Hoheitsgewässer eines Drittstaats verlassen) niemals unvoreingenommen kontrolliert oder analysiert wurden. Die BORTEC-Studie stellt fest: „Obwohl es theoretisch möglich ist, die gesamte Hochsee täglich rund um die Uhr zu überwachen, würde diese Maßnahme untragbar große Ressourcen in Anspruch nehmen, ohne dass der Erfolg dieser Anstrengungen feststünde."[199] Anstatt die technische Eignung des vorgeschlagenen EUROSUR-Systems zweifelsfrei nachzuweisen, hat die Europäische Kommission den Verordnungsvorschlag einfach so allgemein formuliert, dass er jede mögliche Lösung abdeckt. Gleichzeitig wurde die Forschung und Entwicklung für das System an das Europäische Programm für Sicherheitsforschung ausgegliedert (siehe Kapitel 4.2).

Die Technische Studie zu EUROSUR, die das deutsche Rüstungsunternehmen ESG und dessen Subunternehmen EADS, SELEX-Finmeccanica und Thales im Jahr 2010 erstellt haben, zählt 11 verschiedene „Überwachungssensoren" und 18 verschiedene „Seeüberwachungssysteme" auf, die zur Überwachung von Land- und Seegrenzen eingesetzt werden *könnten*.[200] Diese gehören zu den 13 verschiedenen Informationsquellen, die Daten für die nationalen und europäischen Lagebilder liefern werden. Es steht zu befürchten, dass schon allein der Umfang des geplanten Systems dieses für technische Probleme und eine Überschreitung der geplanten Kosten anfällig macht. Auch ist es mehr als bedauerlich, dass sowohl die BORTEC-Studie als auch die Studie von ESG weder dem Europäischen Parlament oder den Parlamenten der Mitgliedstaaten noch der breiten Öffentlichkeit zu einer Überprüfung vorgelegt wurden.

Obwohl sie den Auftrag für die technische Entwicklung von EUROSUR bereits 2008 vergeben hatte, begann die Europäische Kommission erst 2011 mit einer Schätzung der möglichen Kosten und gab bei den Beratungsfirmen GHK, Unysis und EUROCONSULT eine „Technische Studie zur Abschätzung der finanziellen Auswirkungen durch die Einrichtung des Europäischen Grenzkontrollsystems" in

197 SEC (2011) 1536 final, S. 5. [Hervorhebung im Original].

198 Siehe „Death by policy: The fatal realities of 'Fortress Europe' – 15181 deaths", abrufbar unter: http://www.unitedagainstracism.org/pages/campfatalrealities.htm.

199 BORTEC- Studie S. 98.

200 Teilprojekt 1, „Technical and management concepts for the surveillance of land and maritime borders", Technische Studie für die Generaldirektion für Justiz, Freiheit und Sicherheit der Europäischen Kommission, im Rahmen des Europäischen Grenzkontrollsystems (EUROSUR), Januar 2010.

Auftrag.[201] Die Studie sollte für drei Optionen bei der Einrichtung von EUROSUR die Kosten im Zeitraum 2011-2020 einschätzen: (i) eine dezentralisierte Variante, die nur die Systeme der Mitgliedstaaten verknüpft, (ii) eine teilweise zentralisierte Variante, bei der bestimmte Daten zentral durch die Agentur FRONTEX erfasst werden oder (iii) eine vollständige zentralisierte Variante. Die geschätzten Kosten lagen, ohne jährliche Betriebskosten, zwischen 318 Mio. Euro für ein dezentralisiertes EUROSUR bis zu 913 Mio. Euro für das vollständig zentralisierte System. Die bevorzugte Option ist die „teilzentralisierte Variante", bei der die Kosten auf 338,7 Mio. Euro geschätzt wurden (siehe Abbildung 4).[202]

Grundlage der Kostenschätzung waren frühere Schätzungen aus der Technischen Studie zu EUROSUR, eine Befragung der Mitgliedstaaten und konkrete Projekte, die bereits durch den Europäischen Außengrenzenfonds finanziert werden. Ein Viertel der Mitgliedstaaten lieferten keinerlei finanzielle Daten und bei den übrigen „gab es starke Schwankungen bezüglich der Vollständigkeit und Vergleichbarkeit der Daten."[203] Zur Schätzung der Kosten für die Aufrüstung der Nationalen Koordinierungszentren und die Integration von FRONTEX in das System EUROSUR (siehe Abb. 5) betrachteten die externen Beraterfirmen einfach ein oder zwei „Beispielstaaten" für jede politische Option und extrapolierten die Gesamtsumme aus den Schätzwerten der Mitgliedstaaten und der Agentur Frontex.[204] Die Europäische Kommission hätte zugeben müssen, dass die gewonnenen Schätzwerte angesichts des in diesem Ansatz enthaltenen Fehlerspielraums reine Spekulation sind. Dass Entwicklung und Umsetzung von EUROSUR aus dem Europäischen Programm für Sicherheitsforschung bzw. dem Europäischen Außengrenzenfonds finanziert werden, macht es noch schwieriger, die Kosten zu überwachen und Mehrkosten oder Fehlinvestitionen zu erkennen.

201 Technical study assessing the financial impact of establishing the European External Border Surveillance System (EUROSUR), Abschlussbericht, Generaldirektion Inneres, September 2011.

202 SEC (2011) 1536 final, S. 38-39.

203 SEC (2011) 1536 final, S. 36.

204 Für Option 1 wurden die Zahlen aus Belgien und Frankreich verwendet, für Option 2 die Zahlen aus der Slowakei und Zypern und für Option 3 die Zahlen aus Finnland.

Abb. 4: „Politische Optionen“ zur Finanzierung von EUROSUR[205]

Schritt	Komponente	Option x.1	Option x.2	Option x.3	Bevorzugte Optionen	
		Dezentralisierter Ansatz	Teilzentralisierter Ansatz	Zentralisierter Ansatz	Zuständig	Finanzierung
1	**Nationale Koordinierungszentren**	**99,6 Mio.€**	271,6 Mio €	610 Mio €	**Mitgliedstaaten**	**EBF (ISF)**
1	**Frontex-Lagezentrum**	**95,6 Mio €**	129,8 Mio €	137 Mio €	**Frontex**	**Frontex (ISF)**
2,7	**Kommunikationsnetz**	42,4 Mio €	**46,7 Mio €**	49,3 Mio €		
6	**gemeinsames Informationsbild des Grenzvorbereichs**	0,0 €	**29,3 Mio €**	29,2 Mio €		
3	**Netzwerk mit Drittländern**	0,0 €	**5,4 Mio €**	25,3 Mio €	**Mitgliedstaaten**	**DCI, EBF (ISF)**
5	**Gemeinsame Anwendung von Überwachungsinstrumenten**	80,5 Mio €	**62,1 Mio €**	62,3 Mio €	**Frontex EUSC EMSA**	**Frontex GMES**
Gesamt		318,1 Mio €	544,9 Mio €	913 Mio €	**Finanzbogen:**	
Bevorzugte Option		**338,7 Mio € (2011-2020)**			**244 Mio. € (2014-20)**	

Abb. 5: Geschätzte Kosten von EUROSUR: Nationale Koordinierungszentren und FRONTEX[206]

Kosten der politischen Optionen im Vergleich, 2011-2020. In Euro (€) und prozentual (%)

	Basislinie (2007-2010)	Option 1.1: Dezentralisierte Option (2011-2020)	Option 1.2: Übergreifende Option (2011-2020)	Option 1.3: Zentralisierte Option (2011-2020)
Gesamt- NCC kosten	40,054,849	99.697.200 €	271.673.160 €	610.386.216 €
Gesamt- FSC kosten	2,238,499	95.591.020 €	129.824.552 €	136.983.844 €
GESAMT-KOSTEN	**42,293,348**	**195.288.220 €**	**401.497.712 €**	**747,370,060 €**
Anteil MS (%)	95%	51%	68%	82%
Anteil FSC (%)	5%	49%	32%	18%

205 Quelle: SEC (2011) 1536 final, S. 39.
206 Ebd. S. 31.

4.1.2 Einreise-/Ausreisesystem und Registrierungsprogramm für Reisende

Im Jahr 2008 gab die Kommission an, dass „die geschätzten Kosten für das zentralisierte Einreise-/Ausreiseprogramm und das Registrierungsprogramm für Reisende auf 2-3 Jahre gerechnet circa 20 Millionen Euro und die jährlichen Wartungs- und Betriebskosten ungefähr 6 Millionen Euro betragen."[207] Sie schätzte, dass die Kosten für die Einführung von EES und RTP in den Mitgliedstaaten weitere 35 Mio. Euro betragen dürften, „die aber erheblich variieren könnten, je nachdem, wie viele automatische Gates installiert werden. Die Einrichtung eines automatischen Gates schlägt mit etwa 35 000 EUR zu Buche."[208] Die Kommission rechtfertigte die niedrigen Schätzwerte damit, dass keines der beiden Systeme so teuer sei wie das Visa-Informationssystem, „da der technische Aufbau beider Systeme maximale Synergieeffekte mit dem VIS ermöglichen."[209] Wie Peers feststellte, berücksichtigt diese Schätzung offensichtlich nicht die Kosten, die entstehen, wenn das VIS dazu verwendet oder dafür erweitert wird, die Ausreise von Drittstaatenangehörigen an Außengrenzen zu erfassen.[210] Als die Kommission die möglichen Kosten von EES und RTP 2011 neu bewertete, lagen ihre Schätzwerte wesentlich höher: die Entwicklung der zentralen Elemente von EES und RTP könnten in der Größenordnung von 400 Mio. Euro liegen und die jährlichen Betriebskosten in den ersten fünf Jahren bei 180 Mio. Euro. Sofern EES und RTP auf einer gemeinsamen technischen Plattform aufgebaut werden, können nach Schätzung der Kommission bis zu 30 % der Kosten eingespart werden.[211] Die Kommission hat 1,1 Mrd. Euro aus dem geplanten Fonds für innere Sicherheit (ISF) 2014-2020 für Entwicklung und Einführung dieser Systeme veranschlagt (siehe Kapitel 4.3.3).

Die hohen Kosten für die Entwicklung des EES können nur gerechtfertigt werden, wenn die Erforderlichkeit und Angemessenheit des Systems zweifelsfrei bewiesen ist. Es konnte jedoch bisher nicht nachgewiesen werden, dass das Einreise-/Ausreisesystem zur Abschreckung und Erfassung von Personen geeignet ist, die ihre Visafrist überziehen. Wie bereits ausgeführt, *könnte* dieses Ziel erreicht werden, indem man die EES-Warnmeldungen über die Systeme SIS bzw SIS II mit Warnmeldungen an die Polizei verknüpft. Dies ist derzeit aber gesetzeswidrig (und jede Änderung der SIS-Vorschriften müsste durch einen eindeutigen Nachweis der Wirksamkeit und Erforderlichkeit dieser Maßnahme begründet werden). Ob das EES eine Sicherheitsmaßnahme darstellt, lässt sich noch stärker bezweifeln. Ein Aktionsplan der Europäischen Union zum Kampf gegen Terrorismus

207 Die Kommission wäre nach diesem Plan für Beschaffung und Wartung der zentralen Datenbank zuständig (die zentralisierte Datenbank von EES und RTP) und die Mitgliedstaaten für Nebengeräte, wie Fingerabdruckscanner, Geräte zur Speicherung biometrischer Merkmale, (halb-)automatische Grenzkontrollen, spezielle Kontrollwege sowie die für die Anmeldung der registrierten Reisenden benötigten Geräte und Mitarbeiter. SEC (2008) 153, S. 27 und S. 30.

208 SEK (2008) 154.

209 SEC (2008) 153, S. 20. Im Jahr 2004 wurde die Einrichtung eines automatisierten Einreise-/Ausreisesystems an den Außengrenzen der Union im Rahmen der Folgenabschätzung für den Aufbau des VIS behandelt. In diesem Zusammenhang lautete das Urteil, das EES sei „zu teuer und überproportioniert", SEC (2008) 153, S. 24.

210 Wie Peers in seinem Bericht feststellt, „ist es möglich, dass einige Mitgliedstaaten die Infrastruktur zur Anwendung des VIS an manchen Ausreisestellen nicht installieren, da die Mitgliedstaaten nicht zur Verwendung des derzeitigen VIS bei der Ausreise verpflichtet sind. Sollte dies der Fall sein, berücksichtigt der angenommene Status Quo der Kommission nicht alle Kosten für die Einführung eines Einreise-/Ausreisesystems, da dies die Mitgliedstaaten zur Installation der für die vollständige Funktion des Systems erforderlichen Infrastruktur an allen Ausreisestellen verpflichten würde." Steve Peers, „Proposed new border control systems", Themenpapier für das Europäische Parlament, PE 408.296, 25. Juni 2008.

211 KOM (2011) 680 endgültig, S. 10 (basierend auf einer Studie der Kommission von 2010).

nannte ein Einreise-/Ausreisesystem als eine der Maßnahmen, die zu Schutz vor Terrorismus ergriffen werden „könnte“,[212] , die Kommission hat jedoch bereits zugegeben dass „das Potenzial (eines EES) zur Eindämmung von Terrorismus und von Schwerkriminalität nicht signifikant erscheint.”[213]

Abb. 6: Kostenschätzung der Kommission für die Systeme RTP und EES[214]

	Einmalige Entwicklungskosten auf zentraler und nationaler Ebene (3 Entwicklungsjahre) (in Mio. EUR)	Jährliche Betriebskosten auf zentraler und nationaler Ebene (5 Entwicklungsjahre) (in Mio. EUR)	**Gesamtkosten auf zentraler und nationaler Ebene** (in Mio. EUR)
RTP: Option mit Speicherung einer einmaligen Kennnummer in einer Marke und Speicherung von biometrischen Daten und Antragsdaten in einer zentralen Datenbank	207 (MS- 164 - zentral- 43)	101 (MS- 81 - zentral- 20)	**712**
EES: Option mit zentralem System und später erfolgender Erfassung biometrischer Daten	183 (MS- 146 - zentral- 37)	88 (MS- 74 - zentral- 14)	**623**

Außerdem kann ein EES offensichtlich zu wesentlich längeren Warteschlangen für Drittstaatenangehörige führen, die in den Schengenraum einreisen möchten. Bei Drittstaatenangehörigen, die ein Visum für die Einreise benötigen, werden bei der Einreise bereits biometrische Daten erfasst. Personen auf den so genannten „Weißen Listen“, die kein Visum benötigen, sind von der Erfassungspflicht bereit. Wenn man von den Grenzkontrollzahlen ausgeht, die bei einer weitreichenden Überwachungsübung im Jahr 2009 erhoben wurden[215], könnte dies

212 Dokument des Rates 5771, 27. Januar 2006.

213 SEK (2008) 154 endgültig. Die Kommission stellt fest, dass „die Mehrheit der Personen, denen die Einreise verweigert wird, weder Terroristen noch Schwerkriminelle sind, sondern Menschen ohne ordnungsgemäße Reisepapiere, die als mögliche illegale Zuwanderer verdächtigt werden." SEC (2008) 153 final, S. 9. Theoretisch könnte das EES Daten über die Reisen von Drittstaatenangehörigen erfassen, die keiner Visapflicht unterliegen, insbesondere, wenn diese als „verdächtig“ gelten. Nach Angaben der Kommission „könnten derartige Daten über die Bewegungen von Personen, die verdächtigt werden, Terroristen oder Schwerkriminelle zu sein, dazu dienen, deren Aufenthalt zu bestimmen und strafrechtlich zu verfolgen." Wie der Bericht von Steve Peers feststellt, „wenn eine Person, die in den Schengenraum eingereist ist, später einer terroristischen Aktivität verdächtigt wird, besteht mit Hilfe des Einreise-/Ausreisesystems die eingeschränkte Möglichkeit festzustellen, ob (und gegebenenfalls wann und wo) der Verdächtigte den Schengenraum verlassen hat, sofern der Verdächtigte auf legalem Weg aus dem Schengenraum ausreist.“ Peers, „Proposed new border control systems“, S. 9.

214 KOM (2011) 680 endgültig, S. 16.

215 Dokument des Rates 13267/09, 22. September 2009.

dazu führen, dass von weiteren 57 Millionen Drittstaatenangehörige, die auf einer „weißen Liste“ stehen, Fingerabdrücke erfasst werden müssten. Laut Folgenabschätzung für das VIS aus dem Jahr 2004 dauern die Formalitäten bei der Einreise in die USA durchschnittlich 15 Sekunden länger, seit in den Vereinigten Staaten biometrische Daten für das Programm US VISIT erfasst werden. Auch wenn die EU diese Zielvorgabe bei den 57 Millionen Drittstaatenangehörigen erreichen könnte, würde an den Grenzen der Union dadurch jährlich eine zusätzliche Wartezeit von 27 Jahren entstehen. Wie bereits erwähnt, müssten außerdem Regeln für den Umgang mit Falschmeldungen, Personen, bei denen bestimmte biometrische Merkmale nicht erfasst werden können, und zahlreiche weitere Eventualitäten festgelegt werden.

Die Europäische Kommission hat angeführt, dass „diesen derzeit vorgesehenen umfangreichen Kosten auch eine Reihe von Vorteilen gegenüberstünden: Beispielsweise könnte sich infolge des Registrierungsprogramms für Reisende im Verbund mit der Tatsache, dass ein Großteil aller Grenzübergänge automatisiert würde, ein Minderbedarf an Grenzkontrollressourcen von 40 % ergeben, was Einsparungen in Höhe von 500 Mio. EUR jährlich gleichkäme. Selbst bei weniger optimistischen Berechnungen mit einem erwarteten Einsparpotenzial von 250 Mio. EUR jährlich könnte sich für die Mitgliedstaaten schon nach dem zweiten Betriebsjahr eine Nettokostenersparnis ergeben.“[216] Wie diese Einsparungen erreicht werden sollen, wenn man vom gesunkenen Personalaufwand durch die Verwendung automatischer Kontrollgates einmal absieht, wird nicht näher ausgeführt. Und obwohl ein freiwilliges europaweites Registrierungsprogramm für Reisende den registrierten Personen einen weit schnelleren Grenzübertritt ermöglichen würde als nicht registrierten Reisenden, schätzt die Kommission, dass nur 4 bis 5 Millionen Reisende jährlich das System tatsächlich nutzen werden.[217] Schätzungen zufolge macht dies lediglich fünf Prozent der Drittstaatenangehörigen aus, die jährlich die Außengrenzen überqueren. Da die Wartezeiten an den Gates für registrierte Reisende derzeit vor allem deshalb kürzer sind, weil nur relativ wenige Menschen an derartigen Programmen teilnehmen (die normalerweise eine Jahresgebühr von rund 125 Euro erheben), sind ernsthafte Zweifel angebracht, ob diese Kontrollgates den Druck auf die Grenzen des Schengenraums senken oder für eine große Mehrzahl das Reisen vereinfachen können.[218] Die Argumentation für automatisierte Grenzkontrolle würde gestärkt, wenn ihre Benutzung für alle Reisenden, d. h. auch für EU-Bürger, verpflichtend vorgeschrieben wäre. Dies geht jedoch weit über die geplanten Gesetzesvorschläge hinaus.

4.2 Grenzsicherung und das Europäische Programm für Sicherheitsforschung

Die immer öfter geforderte Verwendung neuer Technologien zur Unterstützung der Grenzüberwachungspolitik der Union ist eng mit neuen Ansätzen der „Grenzsicherung“ verbunden, die im Rahmen des Europäischen Programms für Sicherheitsforschung (European Security Research Programme, ESRP) entwickelt werden. Das ESRP wurde 2004 ins Leben gerufen und später in das Forschungsrahmenprogramm der EU „FP7“ integriert, das von 2007 bis 2013 läuft.[219] Das ESRP soll

216 KOM (2011) 680 endgültig, S. 11-12.
217 KOM (2011) 680 endgültig, S. 14.
218 SEC (2008) 153, S. 66.
219 Beschluss der Kommission vom 3. Februar 2004 über die Umsetzung der vorbereitenden Maßnahme zur Stärkung des Industriepotenzials in Europa auf dem Gebiet der Sicherheitsforschung (2004/213/EG). Beschluss Nr. 1982/2006/EG des Europäischen Parlaments und des Rates vom 18. Dezember 2006 über

einerseits die Sicherheit der Bürger/-innen der Europäischen Union verbessern und zweitens die Wettbewerbsfähigkeit der europäischen Sicherheitsbranche auf dem Weltmarkt stärken.[220] Die Europäische Kommission nutzt das ESRP in zunehmendem Maße zur Finanzierung von Projekten, die der technischen Entwicklung des EUROSUR-Systems dienen. Andere Projekte präsentieren Technologien für die Initiative „intelligente Grenzen" oder dienen zur Entwicklung von Systemen für das „Profiling" von Reisenden.

Grenzsicherung ist einer der fünf zentralen „Themenbereiche" des ESRP und gehört schon seit den ersten Anfängen des Programms zu dessen wichtigstem Aufgabenbereich. Im Oktober 2004 veranstaltete die Europäische Kommission ein Seminar im slowenischen Ljubljana zum Thema „Forschung und technologische Hindernisse im Bereich der Grenzüberwachung", an dem politische Entscheidungsträger der EU, Grenzschützer/-innen der Mitgliedstaaten, einige der größten Rüstungsunternehmen Europas, wie Finmeccanica, Thales, EADS und Sagem, sowie der Europäische Verband der Luftfahrt-, Raumfahrt- und Verteidigungsindustrie (eine Interessenverband, der die meisten Sicherheits- und Rüstungsunternehmen Europas vertritt) teilnahmen. Diese Unternehmen waren auch in den Beratergremien vertreten, die die Europäische Kommission zur Beratung der EU im Bereich ESRP eingerichtet hatte, insbesondere in der „Gruppe von Persönlichkeiten im Bereich der Sicherheitsforschung" und im „Europäischen Beirat für Sicherheitsforschung", deren gemeinsamen Vorsitz die Geschäftsführer von Thales und EADS führten.[221] Der Abschlussbericht des Beirats vom September 2006 bestimmte die Prioritäten für den mit „Sicherheit" befassten Teil des Rahmenprogramms FP7.[222]

Im Bereich „Grenzsicherung" waren dies „Technologien zur Erfassung, Identifizierung und Authentifizierung", „Lagebilder und Lagebeurteilung sowie Überwachung" und Datenmanagement, Kommunikation, Ausbildung und Übungen. Zu diesen Prioritätsthemen wurden fünf Forschungsbereiche festgelegt: Hafensicherung (einschließlich Containerhäfen), Überwachung von Seegrenzen, unbewachte Landgrenzen, Grenzkontrollstellen und „erweitere intelligente Grenzen.".[223] Abbildung 7 des Beiratsberichts fasst die Prioritäten im Bereich Forschung und Entwicklung im Rahmen des Teilprogramms „Grenzsicherung" des Rahmenprogramms FP7 anschaulich zusammen. Ein drittes Beratungsgremium für Sicherheitsforschung, das „Europäische Forum für Sicherheitsforschung und Innovation" wurde im Frühjahr 2007 gegründet und beauftragt, eine langfristige Vision für die Tätigkeit des ESRP in den nächsten 20 Jahren zu entwickeln. Die Arbeitsgruppe 3 des Europäischen Forums für Sicherheitsforschung und Innovation befasste sich mit dem Thema „Grenzsicherung".[224] Den Vorsitz hatte Erik Berglund, der Leiter der Forschungs- und Entwicklungsabteilung von FRONTEX, Berichterstatter war der stellvertretende Leiter des Bereichs zivile Anwendung des italienischen Rüstungskonzerns Finmeccanica. Im Abschlussbericht des

---

das Siebte Rahmenprogramm der Europäischen Gemeinschaft für Forschung, technologische Entwicklung und Demonstration (2007 bis 2013).

220 Beschluss 1982/2006/EG, Anhang 1.

221 Hayes, „Neoconopticon: The EU security-industrial complex", TNI/Statewatch (2009): S. 15–17.

222 „Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board", Brüssel, Europäische Kommission, 2006.

223 „Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board", Brüssel, Europäische Kommission, 2006, S. 25.

224 „European security research and innovation forum", Abschlussbericht, Brüssel, Europäische Kommission, 2009.

Europäischen Forums für Sicherheitsforschung und Innovation wurde die Unterstützung der EU-Politik zum integrierten Grenzmanagement sowie die Bereitstellung der dafür benötigten technischen Geräte zu einem Preis, der deren breiten Einsatz erlaubt, als wichtigste Herausforderungen des ESRP benannt.

Erik Berglund, der inzwischen die Abteilung Kapazitätsaufbau der Agentur FRONTEX leitet, gibt offen zu, wie wichtig die Beteiligung an dem ESRP ist. „Wir [FRONTEX] mussten in der Welt da draußen unser Territorium abstecken, wenn wir wirksam arbeiten wollten. Und zu der Zeit war die beste Chance dazu die Beteiligung an der Sicherheitsforschung der EU, die in diesem Jahr gerade wieder ernsthaft in Gang kam."[225] Die Forschungs- und Entwicklungsabteilung von FRONTEX war bald darauf an der Bewertung der für das Rahmenprogramm FP7 eingereichten Forschungsprojekte beteiligt und war in den Beiräten der Endnutzer vertreten, „wo die Agentur die [Projekt-]Entwicklung in ihrem Sinne beeinflussen konnte." Die Agentur veranstaltet heute mindestens zweimal pro Jahr Seminare für Technologieanbieter, in denen die Sicherheitsbranche ihre neuesten Produkte präsentieren kann, und Branchenvertreter aus bestimmten Projekten nehmen regelmäßig an der Umsetzungsgruppe für die Überwachung von Seegrenzen des Programms FP7 teil, deren Vorsitz FRONTEX innehat. Außerdem ist FRONTEX in der 20 Mitglieder starken Beratenden Gruppe für das Sicherheitskonzept (SAG) vertreten, die die Europäische Kommission bei den jährlichen Ausschreibungen für das Europäische Programm zur Sicherheitsforschung berät.[226] Genau wie andere Beobachter hegen auch die Autoren dieses Berichts die Befürchtung, dass die Einrichtung des ESRP die Beziehungen zwischen der Sicherheits- und Rüstungsbranche und den Entscheidungsträgern, die für Entwicklung und Umsetzung der Grenzüberwachung auf EU-Ebene verantwortlich sind, institutionalisiert und gefestigt hat, während gleichzeitig die Stimmen ausgegrenzt wurden, die nicht von der Notwendigkeit einer „intelligenten Überwachung" oder „intelligenter Grenzen" überzeugt sind.[227] So hat eine Studie im Auftrag der Fachabteilung Bürgerrechte und konstitutionelle Angelegenheiten des Europäischen Parlaments im November 2010 festgestellt:

> Wichtigstes Ziel der Maßnahmen der EU im Bereich Sicherheitsforschung- und Entwicklung war es, Vertreter der Verteidigungs- und Innenministerien der Mitgliedstaaten und assoziierten Ländern mit den Vertretern wichtiger Unternehmen der Verteidigungs- und Sicherheitsbranche zusammen zu bringen. Dabei wurden Vertreter der Zivilgesellschaft und der Parlamente sowie Institutionen und Organisationen, die sich für den Schutz der bürgerlichen Freiheiten und Grundfreiheiten einsetzen, wie z. B. Datenschutzbeauftragte und Institutionen zum Schutz der Grundrechte, weitestgehend übergangen. Im Ergebnis hat dies zu einem thematisch stark eingeschränkten Dialog geführt, der die Sicherheitsforschung ausschließlich aus der Perspektive der Sicherheitsbehörden und -dienste sowie die Sicherheitsbranche betrachtet und die Anforderungen ignoriert, die sich aus der Europäischen Union als Raum der Freiheit ergeben.[228]

225 FRONTEX (2010) „Beyond the Frontiers - Frontex: The First Five Years", S. 53, abrufbar unter: http://www.frontex.europa.eu/assets/Publications/General/Beyond_the_Frontiers.pdf

226 In der SAG ist auch die Sicherheitsbranche gut vertreten, siehe die aktuelle Liste der Mitglieder unter: http://ec.europa.eu/research/fp7/pdf/advisory-groups/security-members.pdf#view=fit&pagemode=none

227 Bigo and Jeandesboz, „The EU and the European security industry: Questioning the 'Public-Private Dialogue'", INEX Policy Briefs Nr. 5, CEPS, 2010. Burgess und Hanssen, „Public-private dialogue in security research", Brüssel, Europäisches Parlament, PE 393.286, 2008.

229 „Review of security measures in the Research Framework Programme", Brüssel: Fachabteilung Bürgerrechte und konstitutionelle Angelegenheiten des Europäischen Parlaments, 2010, S. 10.

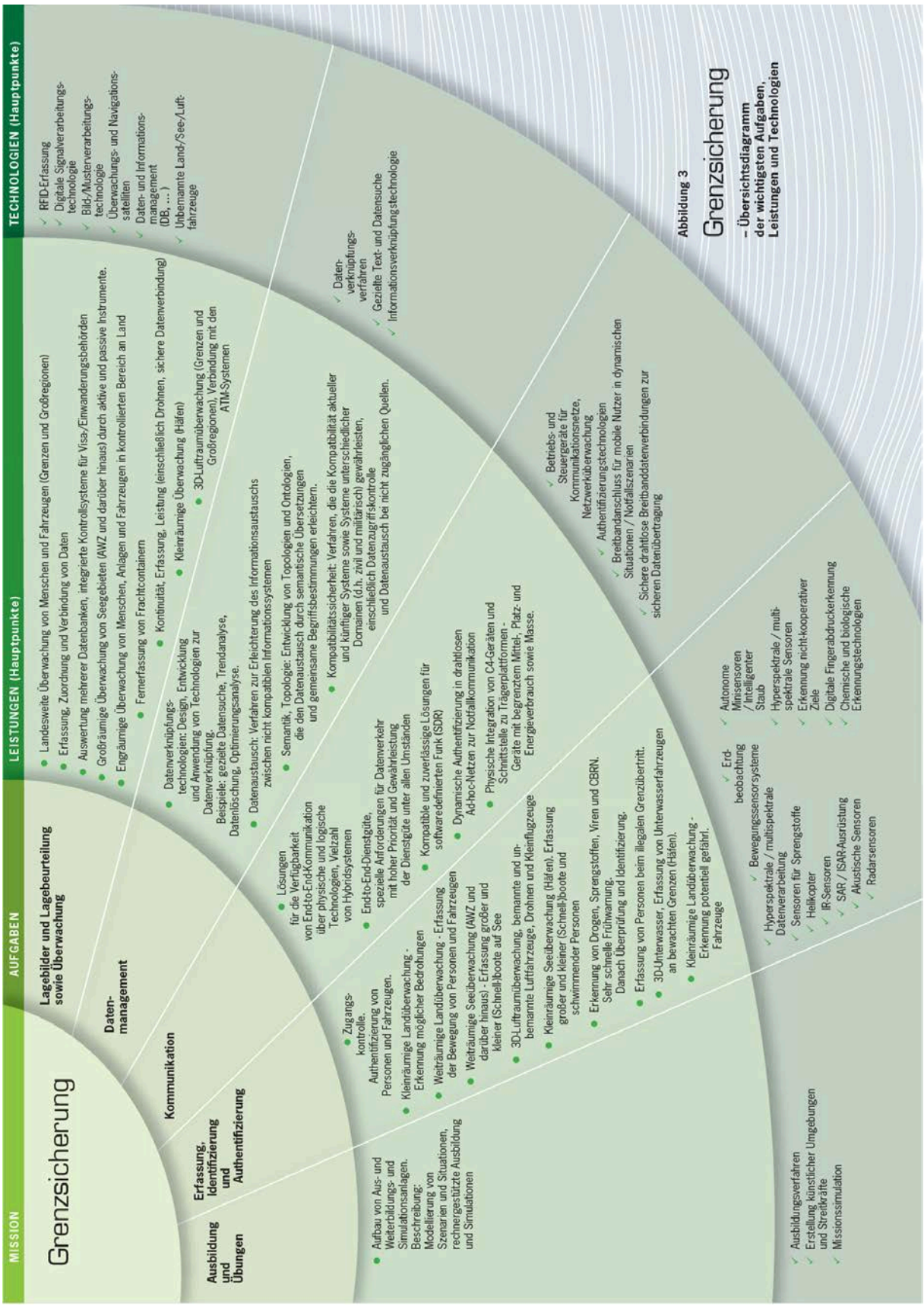


Abb. 7: Wege zur Grenzsicherung in der Europäischen Union[229]

229 „Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board“, Brüssel, Europäische Kommission, 2006, S. 26.

4.2.1 EU-finanzierte Forschungs- und Entwicklungsprojekte für EUROSUR

Forschung, Entwicklung und Erprobung der Komponenten und gemeinsamen Überwachungsinstrumente von EUROSUR wurden an das Europäische Programm für Sicherheitsforschung ausgelagert, mit dessen Hilfe Studien, Forschungs- und Entwicklungsprojekte und Demonstrationen im Bereich Grenzüberwachung und Grenzschutz finanziert wurden. Im Legislativvorschlag der EU zur Einrichtung des Achten Rahmenprogramms für Forschung und Innovation („Horizont 2020", 2014-2020) werden Forschungs- und Entwicklungsprojekte für EUROSUR ausdrücklich als Prioritätsfeld des ESRP eingeführt und dieses Verfahren damit formalisiert.[230] Horizont 2020 soll „die globale Wettbewerbsfähigkeit Europas gewährleisten", und ist „Teil der Anstrengungen zur Schaffung von Wachstum und Beschäftigung in Europa" durch Schaffung einer „Innovationsunion".[231] Allerdings scheint fraglich, ob dieses Programm das richtige Instrument für die Finanzierung von Forschungs- und Entwicklungsprojekten zum Nutzen der Grenzüberwachung der EU darstellt.

Kasten 4 enthält 15 Projekte im Bereich Grenzsicherung, die bisher von der EU mit über 170 Mio. Euro finanziell gefördert wurden. Über die Hälfte dieser Projekte lieferten Ergebnisse, die direkt oder indirekt zur Entwicklung und Umsetzung von EUROSUR genutzt wurden. Bis zum Ablauf der derzeitigen Forschungsrahmenprogramms Ende 2013 werden noch zwei weitere Projekte im Bereich Grenzüberwachung in Auftrag gegeben. In der Ausschreibung von 2011 vergab die EU Aufträge zur „Erhöhung der Zuverlässigkeit von Schiffsmeldesystemen" und zur „Voroperationellen Validierung der gemeinsamen Anwendung von Überwachungsinstrumenten auf EU-Ebene".[232] Die Ausschreibung im Jahr 2012 umfasst die Projekte „Weiträumige Überwachung. Von der Erfassung zur Warnmeldung", „Voroperationelle Validierung an Landgrenzen", „Sensortechnologie zur Blattwerkdurchdringung" und „Mobile Geräte an Landgrenzübergangsstellen".[233] Wenn Horizont 2020 im gleichen Umfang zur Finanzierung von Forschungs- und Entwicklungsprojekten für EUROSUR herangezogen wird wie das aktuelle Europäische Forschungsprogramm zur Sicherheitsforschung, lägen die aufgewendeten Mittel bis 2020 in der Größenordnung von 300-400 Mio. Euro, d. h. weit über der Schätzung der Kommission.

Zwar hat es eine gewisse Logik, dass die EU Forschung und Entwicklung betreibt, die ihre politischen Ziele unterstützt. Allerdings würde eine gesonderte Haushaltslinie für die Forschung und Entwicklung von EUROSUR mit klaren Zielvorgaben eine demokratische Kontrolle und Rechenschaftspflicht erleichtern. Außerdem ist es bedenklich, dass die meisten Empfänger dieser Forschungsgelder bisher große Rüstungs- und Sicherheitsunternehmen sind, die davon profitieren, wenn die Mitgliedstaaten oder die Agenturen der Union später in die von den Unternehmen beworbene Grenzüberwachungstechnologie investieren. Elf der dreizehn im Folgenden beschriebenen Projekte werden bzw. wurden von Rüstungsunternehmen geleitet (siehe Kasten 4). Auch die sieben im nächsten Abschnitt aufgeführten Projekte wurden bzw. werden von großen Verteidigungsunternehmen geleitet. Die Mehrheit der Konsortiumsmitglieder ist aus der Verteidigungsbranche. Es finden sich überall die gleichen Namen, deren Einfluss auf das Forschungsrahmenprogramm gründlich dokumentiert ist.

230 Dokument des Rates 17935/11, S. 81.
231 Siehe Horizont 2020, abrufbar unter: http://ec.europa.eu/research/horizon2020/index_en.cfm?pg=h2020.
232 FP7-SEC-2011-1, 20. Juli 2010.
233 FP7-SEC-2012-1 Orientation Paper, 17. April 2012.

Die Ausgliederung von Design, Entwicklung und Umsetzung des EUROSUR-Systems führt klar zu möglichen Interessenkonflikten (siehe Kasten 4). Außerdem begünstigt dieses Verfahren den Transfer von Technologien, die zu militärischen Zwecken entwickelt wurden, in den (üblicherweise) zivilen Bereich der Grenzkontrolle und Seeraumüberwachung. Dies stellt die Rechtmäßigkeit der Finanzierung von Forschungen mit angeblich doppeltem Verwendungszweck in Frage und beeinflusst gleichzeitig die Wahrnehmung und Kontrolle von Migration. Klar ist jedenfalls, dass EUROSUR zwar drei Ziele verfolgt, nämlich Verhinderung von illegaler Einwanderung, Kampf der grenzüberschreitenden Kriminalität und Rettung von Menschen aus Seenot, die EU jedoch noch keine Forschungsprojekte ausgeschrieben oder finanziert hat, die ausschließlich die Sicherheit erhöhen oder Such- und Rettungseinsätze verbessern. Und obwohl Forschung und Entwicklung dem „Stand der Technik" entsprechen müssen, um für eine Förderung durch die EU in Frage zu kommen, gibt es zu den nachfolgenden beschriebenen Projekten keine aussagekräftigen unabhängigen Bewertungen, die deren Bedeutung für die Entwicklung von EUROSUR oder die Eignung bestimmter Technologien überprüfen.

Kasten 4: EU-Projekte im Bereich Sicherheitsforschung, die EUROSUR zugutekommen

Projektname	Ziel	Start-datum	Dauer	Kosten (EU-Anteil)	Leitung
PERSEUS (Protection of European seas and borders through the intelligent use of surveillance)[234]	(1) Präsentation eines „übergreifenden EU-Meeresüberwachungssystems", das die „bestehenden nationalen Systeme und Plattformen integriert, sie durch innovative Funktionen optimiert und die Erwartungen für EUROSUR 2013 noch übertrifft", (2) Unterstützung der Mitgliedstaaten bei der Entwicklung des Netzwerks Nationaler Koordinierungszentren und Integration von FRONTEX und den Überwachungssystemen der Europäischen Agentur für die Sicherheit des Seeverkehrs (EMSA). Umfasst Anwendungen zur besseren „Entdeckung und Identifizierung von nicht kooperativen bzw. verdächtigen Kleinbooten und niedrig fliegenden Flugzeugen", „optimierte und stärker automatisierte Erfassung von abnormalen Schiffsbewegungen" und „Identifizierung von Gefahren und Verfolgung gemeldeter und nicht gemeldeter Schiffe".	Jan. 2011	4 Jahre	43,7 Mio. € (27,9 Mio. €)	Indra Sistemas
SEABILLA (Sea Border Surveillance)[235]	(1) Entwicklung der Architektur eines kostengünstigen Europäischen Seegrenzenüberwachungssystems für	Juni 2010	45 Monate	15,6 Mio. € (9,9 Mio. €)	SELEX (Finmeccanica)

234 PERSEUS, abrufbar unter: http://www.perseus-fp7.eu/.
235 SEABILLA, abrufbar unter: http://www.seabilla.eu/cms/.

	Weltraum-, Land-, See- und Luftinstrumente einschließlich Altsystemen, (2) Einsatz modernster technologischer Lösungen zur Verbesserung der Überwachungsleistung, (3) Entwicklung und Erprobung wichtiger Verbesserung bei der Erfassung, Verfolgung, Identifizierung und automatischen Bewegungsanalyse aller Schiffstypen, einschließlich schwer erfassbarer Schiffe auf offener See oder in Küstennähe.				
OPARUS (Open Architecture for UAV-based Surveillance System)[236]	(1) Definition einer „offenen Architektur zum Betrieb von unbemannten Bord-Boden-Plattformen zur großflächigen Überwachung von Land und Seegrenzen“ mit dem Ziel der Integration von UAV/Drohnen in EUROSUR unter Berücksichtigung des Legislativvorschlags zur Integration von UAV in den zivilen Luftraum, die derzeit von der Europäischen Kommission und EUROCONTROL (der gesamteuropäischen Organisation zur Koordination der zivilen Luftverkehrskontrolle) ausgearbeitet wird, (2) Erprobung von Drohnenüberwachung, sicheren Datenverbindungen, Kommunikationsnetzen und einer generischen Bodenkontrollstation.	Sept. 2010	18 Monate	14 Mio. € (11,9 Mio. €)	Sagem
I2C (integriertes System für kompatible Sensoren und Datenquelle für die Erfassung von unnormalen Schiffsbewegungen und der gemeinsamen Identifizierung von Bedrohungen) [237]	Kombination von Radar- und Schiffsortungssystemen mit neuen Prototypen und Sensoren zur Bildung eines „wetterunabhängigen Verkehrsüberwachungssystems“ das „kleine Boote“ über ein großes Seegebiet von bis zu 200 Seemeilen orten kann“. Verwendet Daten von „geeigneten Sensorplattformen“ wie Flugzeugen und Patrouillenschiffen, unbemannten Unterwasserfahrzeugen und Zeppelinen, die einen „völlig ruhigen Flug für hochauflösende Beobachtungsqualität und eine Nutzlast von 2 Tonnen für Sensoren und Kommunikationsgeräte“ bieten. Verspricht EUROSUR ein „gemeinsames Verkehrslagebild mit Schiffsortungsdaten über durchgeführte Maßnahmen, Flaggen, Seegangsbedingungen, Vorschriften	Okt. 2010	4 Jahre	16 Mio. € (9,9 Mio. €)	DCNS (Marinewerft)

236 OPARUS, abrufbar unter: http://www.oparus.eu/.
237 I2C-Projekt, # 242340.

	usw.“ und die Fähigkeit „unnormale Schiffsbewegungen zu erkennen und automatische Warnmeldungen für eine Überprüfung durch den Bediener auszugeben."				
EFFISEC (EFFicient Integrated SECurity Checkpoints) [238]	(1) Verbesserung der Sicherheit und Effizienz von Land- und Seegrenzübergangsstellen durch Technologie, (2) Verbessertes Arbeitsumfeld für Grenzkontrolleure, (3) Verkürzung der Wartezeiten an den Grenzen.	Mai 2009	4 Jahre	16,3 Mio. € (10 Mio. €)	Sagem
WIMAAS (Wide maritime area airborne surveillance)[239]	Bereitstellung des Luftraumbausteins für die Seeraumüberwachung zu reduzierten Betriebskosten mit mehr Autonomie und höherer Effizienz durch die Einführung von Luftfahrzeugen mit kaum/keiner Bemannung [Drohnen] (…) Ohne Patrouille keine Kontrolle. Kooperation ist wichtig, aber Luftfahrzeuge sind besonders gut für die weiträumige Seeraumüberwachung geeignet, weil sie Lagebilder großer Bereiche (Betriebszeit, Geschwindigkeit und Fernortung), Umleitung in relevante Gebiete (Bedrohung) und flexible Reaktionen (gegebenenfalls Kontrolle) ermöglichen. WiMA²S entwickelt Konzepte und Technologien für verbesserte Einsatzmöglichkeiten zu geringeren Kosten von bemannten Flugfahrzeugen zur Luftraumüberwachung und optional bemannten Flugfahrzeugen zur Luftraumüberwachung, weil die Gesetzeslage in nächster Zeit den Einsatz von UAV im europäischen Luftraum nicht gestatten wird.	Dez. 2008	3 Jahre	40 Mio. € (27,4 Mio. €)	Thales
ARGUS 3D (AiR Guidance and Surveillance 3D)[240]	Bessere Erfassung bemannter und unbemannter Plattformen durch Verarbeitung genauer Informationen von kooperativen und nicht kooperativen Flugobjekten zur Identifizierung potentieller Bedrohungen (…) Ziel der Forschung ist die Untersuchung, Entwicklung und Umsetzung eines einfachen Prototyps eines preisgünstigen, kompatiblen radargestützten Systems.	Dez. 2009	3 Jahre	49,4 Mio. € (32,6 Mio. €)	SELEX (Finmeccanica)
AMASS	Möglichkeit der Beobachtung und	März	42	5,5 Mio. €	Carl Zeiss

238 EFFISEC, abrufbar unter: http://www.effisec.eu/.

239 WIMA2S, abrufbar unter: http://http://www.wimaas.eu.

240 ARGUS 3D, abrufbar unter: http://www.argus3d.eu/project.

(Autonomous maritime surveillance system)[241]	Sicherung von weiträumigen kritischen Seegebieten zur Verhinderung tatsächlicher und möglicher illegaler Einwanderung und Schmuggel von Drogen, Waffen und illegalen Substanzen. Das Überwachungssystem wird aus autonomen, unbemannten Überwachungsbojen mit aktiven und passiven Sensoren bestehen. Wichtigste Sensoren sind nicht gekühlte Wärmebildkameras, die über Breitbandfunk zu einem Netzwerk zusammengeschlossen sind.	2008	Monate	(3,6 Mio. €)	Optronics
SECTRONIC (Security system for maritime infrastructure, ports and coastal zones)[242]	Entwicklung „eines engräumigen 24-Stunden-Überwachungssystems, das auf Schiffen, Plattformen, Container-/Öl-/Gasterminals oder Häfen verwendet werden kann“ und „alle verfügbaren Beobachtungsinstrumente nutzt (zu Land, zur See, Luftraum, Weltraum (…), deren Daten über eine Steuerungszentrale an Land ausgetauscht werden.	Feb. 2008	4 Jahre	4,1 Mio € (2,8 Mio. €)	Marine & Remote Sensing Solutions Ltd
UNCOSS (Underwater Coastal Sea Surveyor)[243]	Entwicklung eines Instruments zur zerstörungsfreien Überprüfung von Unterwasserobjekten vor allem mit Hilfe von Neutronensensoren.	Dez. 2008	4 Jahre	4,1 Mio. € (2,8 Mio. €)	CEA Kommissariat für Atomenergie und alternative Energien
TALOS (Transportable autonomous patrol for land border surveillance)[244]	Praxistest eines „mobilen, modularen, skalierbaren, autonomen und anpassungsfähigen Systems zum Schutz der europäischen Grenzen“, das „unter der Überwachung von Grenzschützer/-innen fast autonom Maßnahmen zur Verhinderung illegaler Aktionen einleitet." Verwendet Drohnen und unbemannte Landfahrzeuge.	Juni 2008	4 Jahre	19,9 Mio. € (12,9 Mio. €)	PIAP (Polnisches Rüstungs-unternehmen)
CONTAIN (Container Security Advanced Information Networking)	Unterstützung beim Umgang mit Gefahren für die Sicherheit von Containern als Teil eines umfassenden Ansatzes zum Management von Verkehrsnetzen, Entwicklung zusammengehöriger technischer Optionen zur Überwachung und Prüfung, sowie containerinterne Sensoren, Kommunikation und Sicherheitstechnik zur Überwachung der	Okt. 2010	42 Monate	15,6 Mio. € (10 Mio. €)	FOI (Forschungsinstitut der schwedischen Streitkräfte)

241 AMASS project, http://www.amass-project.eu/amassproject/.
242 SECTRONIC, abrufbar unter: http://www.sectronic.eu/.
243 UNCOSS, abrufbar unter: http://www.uncoss-project.org/.
244 TALOS, abrufbar unter: http://talos-border.eu/.

	Containerbewegung und sicherheitsrelevanter Daten in Echtzeit. Bereitstellung von erweiterten Containersicherheitsverfahren für Häfen und Hafengemeinschaftssysteme und nationale und europaweite Sicherheitsdatenbanken.				
GLOBE (European Global Border Environment) [245]	Bereitstellung eines umfassenden Rahmens, für den ein integriertes globales Grenzsicherungssystem entwickelt wird (...), das sich durch die vier Hauptschichten der Grenzkontrolle (Herkunftsland, Transitländer, bewachte und unbewachte Grenzen und Inland) bewegt. Beschrieben als „erste Phase" im Demonstrationsprojekt für EUROSUR.	Juli 2008	12 Monate	15,6 Mio. € (10 Mio. €)	Telvent (Spanisches IT-Unternehmen)
OPERAMAR (kompatible Lösung für das Seesicherheitsmanagement der EU) [246]	Entwicklung der Basis für eine gesamteuropäische Seesicherheitserfassung durch die Erstellung einheitlicher Datenmodelle für einen nahtlosen Datenaustausch, die für mehr Kompatibilität zwischen Instrumenten der Union und der Mitgliedstaaten sorgt, und durch Behebung der Diskrepanzen bei organisatorischen und kulturellen Themen.	März 2008	15 Monate	0,7 Mio. € (0,7 Mio. €)	Thales
STABORSEC (Standards for border security enhancement) [247]	Erstellung eines Verzeichnisses der erforderlichen autonomen Geräte zur Grenzsicherung.	Feb. 2007	18 Monate	0,7 Mio. € (0,7 Mio. €)	Sagem
SOBCAH (Surveillance of Borders, Coastlines and Harbours)[248]	Identifizierung der wichtigsten Bedrohungen für „grüne" und „blaue" Grenzen; Entwicklung der am besten geeigneten architektonischen Lösungen gestützt auf modernste Sensor- und Netzwerktechnologien; korrekte Modellierung der entwickelten Lösung; technische Validierung der entwickelten Lösung, zunächst im Labor und dann im Hafen von Genua (Italien), Erstellung eines entsprechenden Fahrplans.	Feb. 2006	18 Monate	3 Mio. € (2 Mio. €)	Galileo Avionica (Finmeccanica)

245 GLOBE-Projekt, # 218207.

246 OPERAMAR Abschlussbericht, abrufbar unter: http://cordis.europa.eu/search/index.cfm?fuseaction=result.document&RS_LANG=EN&RS_RCN=11485692&q=.

247 STABORSEC-Broschüre, abrufbar unter: ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/straborsec_en.pdf.

248 SOCBAH-Broschüre, abrufbar unter: ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/sobcah_en.pdf.

4.2.2 Weltraumgestützte Grenzüberwachung und der gemeinsame Informationsraum

Das EU-Programm „Globale Umwelt- und Sicherheitsüberwachung“ (GMES) dient der Entwicklung eines europäischen Erdbeobachtungssystems. Auch GMES wird aus dem Haushalt des Forschungsrahmenprogramms FP7 für die Jahre 2007-2013 finanziert und erhält rund 85 Prozent des 1,4 Mio. Euro schweren Raumfahrt-Teilprogramms. Bei Einführung des Programms GMES, damals unter dem Namen Globale *Umweltsicherheits*überwachung, war ausschließlich die Erfassung von Umweltdaten vorgesehen und keine Sicherheits- oder Verteidigungsaufgaben. Aber wie das ESRP wurde auch GMES immer stärker für die Entwicklung des EUROSUR-Systems und des gemeinsamen Informationsraums herangezogen. Für die im Verordnungsvorschlag erläuterte gemeinsame Anwendung von Überwachungsinstrumenten ist daher vorgesehen, dass FRONTEX GMES-Dienste verwendet und über das Satellitenzentrum der Europäischen Union Satellitenbilder privater Anbieter kauft.

In Kasten 5 sind sieben GMES-Projekte aufgeführt, die direkt oder indirekt zur Entwicklung von EUROSUR oder allgemein zur Entwicklung des gemeinsamen Informationsraums beigetragen haben. Bisher hat die Union bereits 36 Mio. € zur Finanzierung dieser Projekte bereitgestellt, obwohl in der Finanzuntersuchung zu EUROSUR für den Zeitraum 2011-2020 ein Gesamthaushalt von knapp über 60 Mio. € angegeben wurde. Das heißt, die Gesamtinvestition für Forschungs- und Entwicklungsprojekte im Rahmen von EUROSUR wurde sowohl in der Finanzuntersuchung als auch in der Folgenabschätzung der Kommission eindeutig zu niedrig geschätzt. Zusätzlich zu den Forschungs- und Entwicklungsprojekten, die aus dem Haushalt FP7 finanziert wurden, hat die Europäische Kommission außerdem zwei Pilotprojekte finanziert, in denen der für die gemeinsame Strategie zur Seeraumüberwachung vorgesehene gemeinsame Informationsraum entwickelt werden sollte. Dies sind die Projekte MARSUNO (mit Schwerpunkt Nordatlantik)[249] und BLUEMASSMED (mit Schwerpunkt Mittelmeer),[250] deren Budget insgesamt mehr als 5 Mio. € beträgt.

Kasten 5: GMES-Projekte, die EUROSUR zugute kommen

Name	Ziel	Start-datum	Dauer	Kosten (EU-Anteil)	Leitung
MARISS (MARitime Security Service)	Integration der Daten des Küstenradars, der Schiffsortungssysteme, Schiffsverkehrmanagementsysteme und automatischen Identifikationssysteme mit den Daten von Flugzeugen und der Erdbeobachtung.	Nov. 2005	10 Monate	n/a	Telespazio (Finmeccanica)
TANGO (Telecomm-unications advanced	Entwicklung, Integration, Erprobung und Bewerbung neuer Satellitentelekommunikations-dienste für die GMES. TANGO ist	Nov. 2006	36 Monate	9,3 Mio. € (5,2 Mio €)	EADS Astrium

249 MARSUNO, abrufbar unter: http://www.marsuno.eu/project/.
250 BLUEMASSMED, abrufbar unter: http://www.bluemassmed.net/.

networks for GMES operations)[251]	das erste Projekt im Rahmen des EU-Rahmenprogramms FP6, das sich der Nutzung von Satellitenkommunikation für die Bedürfnisse der gesamten GMES-Gemeinschaft widmet. Das Projekt entwickelt wichtige Umwelt- und Sicherheitsan-wendungen.				
LIMES (Land and sea integrated monitoring for European security)[252]	Definition und Entwicklung von Informationsdienstprototypen auf Basis von Satellitentechnologie zur Unterstützung des Sicherheitsmanagements in der Union und weltweit zu folgenden Zwecken: Organisation und Verteilung von humanitärer Hilfe und Aufbauhilfe; Überwachung der EU-Grenzen (Land und See); Überwachung und Schutz des Seetransports sensibler Fracht, Schutz vor Bedrohungsszenarien (z. B. Terrorismus, Menschenhandel, Verbreitung von Massenvernichtungswaffen).	Dez. 2006	42 Monate	21,2 Mio. € (11,9 Mio. €)	Telespazio (Finmeccanica)
GMOSAIC (GMES services for management of operations, situation awareness and intelligence for regional crises)[253]	Identifizierung und Entwicklung von Produkten, Methoden und Musterdiensten für die Bereitstellung von Geoinformationen für die Außenpolitik der EU und Nachweis der Nachhaltigkeit der globalen Sicherheitsperspektive der GMES.	Jan. 2009	39 Monate	15,2 Mio. € (9,6 Mio. €)	E-GEOS Spa (Telespazio-Finmeccanica)
NEREIDS (Neue Dienstleistungen für die integrierte und hochtechno-logische Seeraumüber-wachung)[254]	Verbesserte Erdbeobachtung durch Kombination mehrerer Sensoren mit innovativen Daten-verknüpfungsverfahren; modularer Ansatz zur Ermöglichung von Datenaustausch und Erstellung eines gemeinsamen Seelagebilds.	Juni 2011	36 Monate	6 Mio. € (4 Mi. €)	GMV Defence & Security
SIMTISYS	Seeraumüberwachung zu	Juni	30	2,5 Mio.	Thales

251 TANGO, abrufbar unter: http://www.teladnetgo.eu/.

252 LIMES-Broschüre, abrufbar unter: http://www.fp6-limes.eu/uploads/docs/LIMES-PRS.004-TPZ%20%5BInfosheet%5D.pdf.

253 GMOSIAC, abrufbar unter: http://www.gmes-gmosaic.eu/.

254 NEREIDS, abrufbar unter: http://www.nereids-fp7.eu/.

(Simulator for Moving Target Indicator System)[255]	Sicherheitszwecken, wie Grenz-überwachung, Verkehrssicherheit, Fischereikontrolle sowie Umwelt-schutz und – überwachung, Verfolgung von kleinen Schiffen.	2011	Monate	€ (1,6 Mio. €)	Alenia
DOLPHIN (Development of Pre-operational Services for Highly Innovative Maritime Surveillance Capabilities) [256]	Entwicklung von Schlüssel-technologien und Innovationen, die Einsatzmängel beheben für die mittelfristige Einführung einer umfassenden und nachhaltigen Nutzung der Erdbeobachtungs-satelliten für die Seeraum-überwachungsziele der EU und der Mitgliedstaaten. DOLPHIN hat das Ziel, neue Instrumente zur effektiven Verbesserung der derzeitigen Seeraumüberwachung zu entwickeln.	Juni 2011	30 Monate	7,1 Mio. € (4 Mio. €)	E-GEOS Spa (Telespazio-Finmeccanic a)

4.2.3 EU-finanzierte Forschungs- und Entwicklungsprojekte für die „intelligenten Grenzen“

Während im Rahmen des EUROSUR-Systems bereits die oben angeführten Projekte durchgeführt wurden, fängt die Europäische Union gerade erst an, die Forschung- und Entwicklung für die Initiative „Intelligente Grenzen" zu finanzieren. Im April 2010 wurde beispielsweise das auf vier Jahre angelegte Projekt TASS (Total Airport Security System) angestoßen, das von dem israelischen Konzern Verint Systems geleitet wird. Das Projekt hat ein Budget von 15 Mio. €, zu dem die EU bisher 9 Mio. € beigesteuert hat. Im Rahmen des Forschungsprogramms FP7 wurden für das Jahr 2011 ausdrücklich Projekte zur Förderung eines Registrierungsprogramms für Reisende und einer automatischen Grenzkontrolle ausgeschrieben. Vermutlich werden ein oder zwei große Erprobungsprojekte finanziert. Es ist bedauerlich, dass die Europäische Kommission beträchtliche Finanzmittel für Forschungs- und Entwicklungsprojekte bereitstellt, bevor überhaupt klar ist, ob die Mitgliedstaaten diesem Ansatz zustimmen und überhaupt ein Registrierungsprogramm für Reisende einrichten wollen.

255 SIMTISYS-Broschüre, abrufbar unter: http://ec.europa.eu/enterprise/policies/space/files/simitisys_en.pdf.
256 DOLPHIN, abrufbar unter: http://www.gmes-dolphin.eu/.

4.3 Finanzierung der Umsetzung von EUROSUR und „intelligenten Grenzen“

Die Europäische Kommission hat jedoch nicht nur das Forschungsprogramm der EU zur Finanzierung von Forschungs- und Entwicklungsprojekten zugunsten der Initiativen „Intelligente Grenzen“ und EUROSUR verwendet, sondern auch mit Hilfe zweier eigenständiger Finanzierungsprogramme, dem Außengrenzenfonds und dem Programm für Migrationszusammenarbeit des Finanzierungsinstruments für die Entwicklungszusammenarbeit, die Umsetzung des EUROSUR-Systems in den Mitgliedstaaten und in Drittländern finanziert. Für 2013 ist geplant, diese Finanzierungsinstrumente zu dem 4,7 Mrd. Euro umfassenden Fonds für die innere Sicherheit (2014-2020) zusammenzufassen.

4.3.1 Der Europäische Außengrenzenfonds

Die Mitgliedstaaten konnten in den vergangenen vier Jahren Mittel aus dem Außengrenzenfonds (EBF) abrufen, um die nationalen Koordinierungszentren einzurichten oder umzubauen, die für die Teilnahme an EUROSUR benötigt werden. Im August 2007 verabschiedete die Europäische Kommission strategische Leitlinien zur Einrichtung des 1,8 Mrd. € schweren Außengrenzenfonds (EBF, 2007-2013), zu dessen Prioritäten die „Unterstützung für den Aufbau (…) der nationalen Komponenten eines europäischen Außengrenzenüberwachungssystems“ gehört.[257] Eine Beratung im Europäischen Parlament fand nicht statt (der Vorschlag für den EUROSUR-Fahrplan wurde dem Parlament erst sechs Monate später vorgelegt).

Beinahe die Hälfte der für den EBF von 2007 bis 2013 veranschlagten 800 Mio. Euro sind für drei Prioritätsbereiche vorgesehen: „Verbesserung der [nationalen] Grenzüberwachungskapazitäten in Bezug auf Infrastruktur und Ausrüstung“, „Schaffung nationaler Koordinierungszentren“ und „Vernetzung und Integration der vorhandenen Kommunikationssysteme zu einem umfassenden Überwachungssystem“.[258]

Die vorliegenden Daten zur Anwendung des Außengrenzenfonds reichen nicht aus, um die Höhe der Mittel zu schätzen, die bisher für EUROSUR aufgewendet wurden. In der Finanzuntersuchung zu EUROSUR wurden die Kosten für „Einrichtung, Ausbau und Instandhaltung“ der nationalen Koordinierungszentren für den Zeitraum 2011-2016 jedoch auf 194 Mio. Euro geschätzt (siehe Abb. 8). In der Folgenabschätzung der Europäischen Kommission aus dem Jahr 2011 betrugen die geschätzten Kosten für die NKZ im Zeitraum 2011-2020 jedoch lediglich 99,6 Mio. Euro, wobei noch einmal derselbe Betrag für das FRONTEX-Lagezentrum veranschlagt wurde. Der EUROSUR-Verordnungsvorschlag sieht jedoch vor, dass Mittel in Höhe von 112 Mio. Euro für die nationalen Lagezentren aus dem Fonds für innere Sicherheit 2014-2020 aufgewendet werden und im gleichen

257 Entscheidung der Kommission 2007/599/EG (strategische Leitlinien für den EBF, Priorität Nr. 2). Siehe auch Entscheidung der Kommission mit Durchführungsbestimmunen für den EBF und Entscheidung 2010/69/EU mit der die Rechtsvorschriften von 2008 geändert und die Finanzierung der Infrastruktur der Mitgliedstaaten ermöglicht wurde.

258 KOM (2011) 857 endgültig, S. 11.

Zeitraum weitere 132 Mio. Euro für das FRONTEX-Lagezentrum und das gemeinsame Lagebild zum Grenzvorbereich (von denen rund zwei Drittel aus dem Fonds für innere Sicherheit stammen).[259]

Abb. 8: Kosten für Einrichtung, Ausbau und Instandhaltung der NKZ 2011–2026[260]

Land	2011	2012	2013	2014	2015	2016	Total
NO	€ -	€ -	€ -	€	€ -	€	€ -
BE	€ 400.000	€ 400.000	€ 400.000	€ 400.000	€ 400.000	€ 400.000	€ 2.400.000
BG	€ 100.000	€ 112.500	€ 125.000	€ 137.500	€ 150.000	€ 162.500	€ 787.500
CY	€ 955.000	€ 1.015.000	€ 1,115.000	€ 1.120.000	€ 1.130.000	€ 1.150.000	€ 6.485.000
DK	€ -	€ -	€ -	€ -	€ -	€ -	€ -
EE	€ 140.000	€ 200.000	€ 250,000	€ 250.000	€ 275,000	€ 275.000	€ 1.390.000
FI	€ 1.825.530	€ 1.916.807	€ 2.000.000	€ 2.113.279	€ 2.812.343	€ 2.952.960	€ 13.620.919
FR	€ 438.100	€ 430.000	€ 430.000	€ 430.000	€ 430.000	€ 430,000	€ 2.588.100
DE	€ -	€ -	€ -	€ -	€ -	€ -	€ -
EL	€ -	€ 1.350.000	€ 6.600.000	€ 2.400.000	€ 2.400.000	€ 2.950.000	€ 15.700.000
HU	€ 81.971	€ 120.610	€ 113.709	€ 113.709	€ 113.709	€ 113.709	€ 657.418
IT	€ 15.338.670	€ 13.741.769	€ 13.531.769	€ 13.531.769	€ 13.131.769	€ 12.993.360	€ 82.269.106
LT	€ 263.297	€ 263.297	€ 263.297	€ 254.609	€ 254.609	€ 254.609	€ 1.553.718
LV	€ 87.763	€ 1.501.240	€ 1.275.697	€ 773.504	€ 773.504	€ 773.504	€ 5.185.212
MT	€ 1.107.000	€ 5.960.000	€ 4.050.000	€ 3.550.000	€ 2.054.000	€ 2.054.000	€ 18.775.000
NL	€ 607.000	€ 607.000	€ 607.000	€ 607.000	€ 607.000	€ 607.000	€ 3.642.000
PO	€ 228.931	€ 228.931	€ 228.931	€ 228.931	€ 228.931	€ 228.931	€ 1.373.585
PT	€ -	€ -	€ -	€ -	€ -	€ -	€ -
RO	€ 3.250.000	€ 1.750.000	€ 750.000	€ 1.750.000	€ 750.000	€ 750.000	€ 9.000.000
SI	€ 120.000	€ 220.000	€ 670.000	€ 570.000	€ 230.000	€ 180.000	€ 1.990.000
SK	€ 928.600	€ 942.800	€ 1.036.460	€ 1.597.006	€ 1.200.687	€ 1.169.775	€ 6.875.328
ES	€ 2.512.090	€ 11.764.842	€ 1.325.537	€ 1.303.729	€ 1.339.390	€ 1.376.100	€ 19.621.688
SE	€ -	€ -	€ -	€ -	€ -	€ -	€ -
Gesa	**€ 28.383.951**	**€ 42.524.795**	**€ 34.772.400**	**€ 31.131.036**	**€ 28.280.942**	**€ 28.821,448**	**€ 193.914.573**

4.3.2 Das Finanzierungsinstrument für die Entwicklungszusammenarbeit

Eines der wichtigsten Ziele von EUROSUR ist die Einbindung der bereits bestehenden regionalen Überwachungssysteme zum Schutz der Grenzen und der inneren Sicherheit in das EUROSUR-Netz. Insbesondere sollen die operativen Daten der Netze SEAHORSE ATLANTIC,[261] Baltic Sea Regional

259 KOM (2011) 873 endgültig, S. 38.

260 Quelle: SEC (2011) 1538 final, S. 35.

261 SEAHORSE ATLANTIC ist ein Zusammenschluss der mit grenzpolizeilichen Aufgaben betrauten Behörden in Spanien, Portugal, Mauritanien, Marokko, dem Senegal, Gambia, Guinea Bissau und Kap Verde zum Austausch von Informationen über „irreguläre Migration und Kriminalität“ an den Küsten von Nord- und Westafrika und den Küsten der Kanarischen Inseln.

Border Control,[262] und Black Sea Border Coordination[263] in EUROSUR integriert werden. Zwischen 2007 und 2010 lagen die Kosten für Ausbau und Instandhaltung der technischen Infrastruktur für diese und ein drittes Zentrum zur regionalen Zusammenarbeit der baltischen Staaten bei 77 Mio. Euro.[264]

Für den Zeitraum 2011-2013 veranschlagt die Europäische Kommission „zwischen 15 und 25 Prozent" des 179 Mio. Euro schweren „Thematic programme for cooperation with third countries in the areas of migration and asylum" [Themenprogramm für Zusammenarbeit mit Drittländern in den Bereichen Migration und Asyl], das einen Teil des Finanzinstruments zur Entwicklungszusammenarbeit EUROPAID darstellt, für „Drittländer an den südlichen und südöstlichen Seegrenzen (…), die einer Zusammenarbeit im Rahmen von EUROSUR zustimmen"[265] Dies übersteigt bei weitem die 5 Mio. Euro, die nach Schätzungen der Kommission für die Eingliederung von Drittländern und regionalen Netzwerken benötigt werden. 2011 legte das spanische Innenministerium einen Vorschlag zur Einrichtung von SEAHORSE MEDITERRANEAN nach dem Modell des Netzwerks SEAHORSE ATLANTIC mit Mitteln des Themenprogramms EUROPAID vor.[266] Abgesehen davon, dass der Austausch von Daten mit Drittländern ohne entsprechende Menschenrechtsstandards bedenklich erscheint, lässt sich auch die Verwendung von Mitteln aus dem Entwicklungshilfehaushalt der EU für die Umsetzung der eigenen sicherheitspolitischen Ziele beklagen. Wie schon andere Beobachter festgestellt haben, kann dies auch die Rechte der Menschen beschränken, ein Land zu verlassen, um anderswo Asyl zu beantragen.[267]

4.3.3 Der Fonds für innere Sicherheit

Laut Vorschlag der Europäischen Kommission sollen 3,5 Mrd. Euro aus dem 4,7 Mio. Euro umfassenden Fonds für innere Sicherheit im Zeitraum 2014-2020 in den Bereich Außengrenzen und Visa und dabei auch in IT-Großsysteme fließen.[268] Zu den Prioritäten des Fonds gehören die „Weiterentwicklung eines integrierten Grenzmanagementsystems durch Erneuerung und Anpassung der in den Bereichen Visum und Grenzen eingesetzten Geräte bzw. der entsprechenden Infrastruktur entsprechend den neuen technischen Entwicklungen. Dazu wird insbesondere die Stärkung der operativen Kapazitäten der Mitgliedstaaten im Rahmen der Standards des Europäischen Grenzüberwachungssystems (EUROSUR) gehören." Wie bereits erwähnt könnten nach Angaben der Kommission 200 Mio. Euro dafür bereitgestellt werden, die Entwicklung der NKZ und des FSC zu unterstützen.

---

262 Die Baltic Sea Region Border Control Cooperation (BSRBCC) ist ein Zusammenschluss der Koordinierungszentren von Estland, Dänemark, Finnland, Deutschland, Lettland, Litauen, Polen, Schweden, Norwegen und Russland.

263 Das Black Sea Border Information Center mit Sitz im bulgarischen Burgas ist eine Initiative des Black Sea Cooperation Forum, zum dem sich die Grenzschützer/-innen Bulgariens, Rumäniens, der Ukraine, Russlands, Georgiens und der Türkei zusammengeschlossen haben.

264 Quelle: SEC (2011) 1538 final, S. 55.

265 Entscheidung der Kommission OJ C 2011/2304 vom 7. April 2011; siehe auch SEC (2011) 1536 final, S. 17.

266 SEAHORSE-Präsentation, abrufbar unter: http://www.imp-med.eu/En/En/image.php?id=125.

267 „Analyse der externen Dimension der Asyl- und Einwanderungspolitik der EU – Synthese und Empfehlungen für das Europäische Parlament", Brüssel, GD externe Politikbereiche der Union, PE 374.366 (2006), S. 12-13.

268 KOM (2011) 750 endgültig, 15. November 2011.

Der ISF soll auch zur

> „Stärkung der Zusammenarbeit mit Drittstaaten eingesetzt werden sowie zur Verstärkung bestimmter Schlüsselaspekte der Grenzüberwachungs- und -managementkapazitäten in Bereichen, die von besonderem Interesse für die EU sind und die unmittelbare Auswirkungen in der EU haben. Beispielsweise könnten im Rahmen von EUROSUR Mittel bereitgestellt werden, um Systeme und Infrastrukturen von Drittstaaten mit denen der EU zu verbinden und damit einen regelmäßigen Informationsaustausch zu ermöglichen."[269]

„Unbeschadet der künftigen Kommissionsvorschläge zu dem Paket „Intelligente Grenzen" und des darauf folgenden Beschlusses des Europäischen Parlaments und des Rates" hat die Europäische Kommission außerdem beinahe ein Drittel des ISF für die Umsetzung dieser Vorschläge veranschlagt.[270] „Die Entwicklungskosten der zentralen und der nationalen Systeme für EES und RTP werden (…) mit 1 bis 1,3 Mrd. EUR veranschlagt(...) .Aufgrund dieser Prämissen und in der Annahme, dass die Entwicklung erst ab 2015 beginnt, wird vorgeschlagen, für diese beiden Systeme im Rahmen dieses Vorschlags (…) 1,1 Mrd. EUR vorzusehen."[271] Es ist bedauerlich, dass die Umsetzung der Vorschläge zu EUROSUR und der Initiative „intelligente Grenzen" praktisch in ein allgemeines Finanzierungsinstrument ausgelagert wurde. Zumindest im Fall der geplanten Systeme EES und RTP wäre die neu eingerichtete Europäische Agentur für IT-Großsysteme für die neuen Projekte verantwortlich. Was EUROSUR betrifft, wurde eine Zuständigkeit der Agentur aus Gründen der politischen Opportunität ausdrücklich ausgeschlossen. Es ist zumindest zweifelhaft, ob FRONTEX oder die Europäische Kommission über die zur Durchführung eines derart ehrgeizigen Vorschlags erforderlichen Erfahrungen oder Kenntnisse verfügen.

Abb. 9: Kritische Analyse der für EUROSUR veranschlagten Kosten

Kosten	**Schätzung der Kommission**	**Unsere Schätzung**	**Berechnungsgrundlage**
Nationale Koordinierungszentren	99,6 Mio. €	227 Mio. €	Geschätzte Kosten der MS von 105 Mio. € für 2011-2013 (siehe Abb. 8) zzgl. 112 Mio. € Zuweisung aus dem ISF 2014-2020 im EUROSUR-Verordnungsvorschlag.
FRONTEX Lagebild & gemeinsames Informationsbild zum Grenzvorbereich	129 Mio. €	152 Mio. €	Geschätzte Kosten für FRONTEX von 20 Mio. € für 2011-2013 (laut Folgenabschätzung der Kommission) zzgl. 132 Mio. € Zuweisung aus dem ISF 2014-2020 im EUROSUR-Verordnungsvorschlag.
Kommunikationsnetz	46,7 Mio. €	46,7 Mio. €	

269 KOM (2011) 749 endgültig, 15. November 2011, S. 9.
270 KOM (2011) 750 endgültig, S. 9.
271 Ebd. S. 8-9.

Gemeinsame Anwendung von Überwachungsinstrumenten	29,6 Mio. €	350 Mio. €	Rund 35 Mio. € jährlich für Forschungs- und Entwicklungsprojekte für EUROSUR in 2010-2012, hochgerechnet auf 10 Jahre. Dabei ist zu beachten, dass Forschung- und Entwicklung für EUROSUR im Programm Horizont 2020 ausdrücklich als Priorität genannt ist und für Sicherheit insgesamt eine Budgeterhöhung vorgesehen ist.
Netzwerke mit Drittländern	5,4 Mio. €	98 Mio. €	2011-2013 jährlich rund 38 Mio. € aus dem Themenbereich Migration des Fonds für Entwicklungszusammenarbeit, hochgerechnet auf 10 Jahre. Die Mittel für die Eingliederung von Drittländern in EUROSUR sollen ab 2014 aus dem ISF kommen.
Gesamt	**338,7 Mio. €**	**873,7 Mio. €**	

4.4 Erfahrungen der Vereinigten Staaten mit SBInet und US VISIT

Es ist bedauerlich, dass die Europäische Kommission bei ihren Folgenabschätzungen zu EUROSUR, dem Einreise-/Ausreisesystem und dem Registrierungsprogramm für Reisende offenbar nicht die Erfolge und Misserfolge vergleichbarer Großprojekte zur Grenzkontrolle in den Vereinigten Staaten berücksichtigt hat. Das geplante EES ähnelt dem Programm US VISIT, das biometrische Daten aller einreisenden Personen erfasst. US VISIT wurde 2004 eingerichtet und speicherte anfänglich von allen Personen, die für die Einreise in die USA ein Visum benötigen, zwei Fingerabdrücke. 2009 speicherte das Programm bereits alle zehn Fingerabdrücke und umfasst nun auch die Angehörigen von Staaten, für die keine Visapflicht galt, einschließlich der Bürger der EU. Wie Peers feststellt,

> enthält die Folgenabschätzung der Kommission von 2008 keine Angaben dazu, wie viele Personen voraussichtlich mit Hilfe eines Einreise-/Ausreisesystems in der EU ausfindig gemacht werden, oder wie vielen Personen aufgrund des Systems ein Visum bzw. an der Grenze die Einreise verweigert wird. Derartige Schätzungen sind jedoch unerlässlich, um den Mehrwert eines solchen Systems zu bewerten. Der Europäische Datenschutzbeauftragte hat darauf hingewiesen, dass das US-System zum Preis von 1,5 Mrd. Dollar die Zurückweisung von 1300 einreisenden Personen an der Grenze ermöglicht hat. Das macht 1 Mio. Dollar pro verweigerte Einreise - obwohl nicht auszuschließen ist, dass das US-System zu weiteren Erfolgen im Bereich der Einwanderungskontrolle geführt hat.[272]

Von den hohen Kosten abgesehen ist es der USA auch nicht gelungen, das Programm US VISIT zu vollenden, das eigentlich neben der Einreise auch die Ausreise aller ausländischen Staatsangehörigen verzeichnen sollte. 2009 stellte der US-amerikanische Rechnungshof (GAO) fest, dass das Ministerium für Innere Sicherheit der Vereinigten Staaten „über keinen detaillierten Plan zur Umsetzung der Ausreisefunktion verfügte und unter anderem die Kostenvoranschläge für die damals vorgeschlagene Ausreiselösung unzuverlässig waren. Es gab kein wirksames Risikomanagement und

272 Peers, „Proposed new border control systems“, S. 9.

die Arbeitsaufgaben des Programms wurden wiederholt geändert." Zweieinhalb Jahre später gibt es immer noch keine erkennbaren Fortschritte bei der Einführung einer funktionsfähigen Ausreisekomponente für das Programm US VISIT.

Die Analyse der Erfahrungen der Vereinigten Staaten mit der 3,7 Mrd. Dollar teuren Secure Border Initiative (SBInet) fällt ebenfalls ernüchternd aus. SBInet wurde 2006 zur Errichtung eines „virtuellen Grenzzauns" mit Hilfe eines komplexen Netzes von hochtechnologischen Überwachungssystemen eingeführt, mit dem die gesamte Nordgrenze (zu Kanada) und Südgrenze (zu Mexiko) kontrolliert werden sollte. Die Finanzierung des Projekts wurde jedoch im Jahr 2010 eingefroren. Vor dem Kongress beschrieb die Ministerin für Innere Sicherheit Janet Napolitano das Projekt als „vom ersten Tag an durch Probleme belastet (…). Keine Frist wurde eingehalten, die operativen Funktionen wurden nicht erreicht und es leistet nicht das, was wir brauchen."[273] 2008 betonte der US-Rechnungshof GAO, mit welchen Problemen SBInet zu kämpfen hat:

> Wichtige Aspekte von SBInet bleiben verschwommen und verändern sich ständig. Aus diesem Grund ist nicht klar und nicht sicher, welche technologischen Möglichkeiten es bieten wird, wann und wo es sie bieten wird und wie es sie bieten wird. So werden beispielsweise seit Projektbeginn Änderungen bei Verwendung und Aufgaben des geplanten SBInet vorgenommen, Punkte die immer noch nicht geklärt sind. Außerdem hat die Projektleitung keinen bewilligten umfassenden Masterplan, an dem sich die Durchführung des Programms orientieren könnte und die soweit das GAO die verfügbaren Informationen zur Kenntnis genommen hat, zeigen diese, dass der Plan laufend geändert wurde. Dieses Risiko aufgrund der Planungsunsicherheit wird noch dadurch verschärft, dass auch kein Ansatz klar festgelegt ist, mit dessen Hilfe SBInet definiert, entwickelt, beschafft, erprobt und verwendet werden soll.[274]

Obwohl noch Elemente des Programms SBInet fortgesetzt werden, ist zu beachten, dass zwar das System des GOA in der Vereinigten Staaten die kritische Prüfung von Projekten wie SBInet und US VISIT durch unabhängige Fachleute ermöglicht, es aber ein vergleichbares Organ zur Überwachung der Sicherheitstechnologieprojekte der EU nicht gibt. Das GAO erstellt ausführliche Berichte, in denen die Ergebnisse und Misserfolge von IT-Großprojekten mit deren Kosten und vorab festgelegten Zielen verglichen werden.[275] Wenn die EU sich entscheidet, ihre eigenen Initiativen für „intelligente Grenzen" weiter voranzutreiben, müssen unbedingt strikte Verfahren zur demokratischen Überwachung und Kontrolle eingeführt werden, insbesondere bezüglich des Systems EUROSUR.

---

273 Defence Industry Daily, 16. Januar 2011.

274 GAO, „Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment", September 2008, S. 2

275 Siehe auch die folgenden Berichte des GAO: „US-VISIT has not fully met expectations and longstanding program management challenges need to be addressed", 16. Februar 2007; „Key US-VISIT components at varying stages of completion, but integrated and reliable schedule needed", November 2009; „Technology deployment delays persist and the impact of border fencing has not been assessed", 9. September 2009; „Despite progress, DHS continues to be challenged in managing its multi-billion dollar annual investment in large-scale information technology systems", 15. September 2009.

5 Zusammenfassung

Es sind inzwischen über vier Jahre vergangen, seit die Europäische Kommission im Jahr 2008 ihr Paket für „intelligente Grenzen“ öffentlich vorgestellt hat. Das Europäische Parlament und der Rat haben die Verhandlungen zum Legislativvorschlag für EUROSUR aufgenommen; in den nächsten Monaten dürfte die Kommission ihre Legislativvorschläge zum Einreise-/Ausreisesystem und zum Registrierungsprogramm für Reisende vorlegen. Da diese drei Systeme im Europäischen Parlament sowie unter den Mitgliedstaaten im Ministerrat der EU kaum behandelt wurden, steht zu befürchten, dass deren voraussichtliche Kosten und Wirksamkeit sowie ihre Auswirkungen auf die Grundrechte nicht angemessen erörtert und durchdacht wurden. Die von der Kommission erstellten Folgenabschätzungen konnten nicht nachweisen, dass die geplanten Systeme für eine wirksame Kontrolle der Einwanderung, eine Erhöhung der Sicherheit der EU-Bürger oder eine erleichterte Ein- und Ausreise von Drittstaatenangehörigen erforderlich sind. Da diese Rechtfertigungen fehlen, bestehen große Zweifel an der Verhältnismäßigkeit von EUROSUR, EES und RTP.

In vielerlei Hinsicht beziehen sich die schwersten Bedenken bezüglich der drei geplanten Systeme jedoch auf den allgemeinen politischen Kurs der EU. Der „Gesamtansatz für Migration und Mobilität“ der EU sieht ausdrücklich die Externalisierung der Einwanderungskontrolle der EU vor. Zu diesem Zweck sollen „Pufferzonen“ außerhalb der EU eingerichtet werden. Außerdem soll durch Zusammenarbeit mit Drittländern die Abreise von Migrant/-innen und Flüchtlingen in Richtung Europa verhindert werden. Menschenrechtsorganisationen stellen die Rechtmäßigkeit dieser Politik in Frage und argumentieren, dass sie „Push-back“-Einsätze erleichtert, welche die Verpflichtungen der EU gemäß den Genfer Konventionen umgehen und gegen den Grundsatz der „Nichtzurückweisung“ verstoßen, der die Abschiebung in Länder, in denen die Betroffenen von Folter und unmenschlicher oder erniedrigender Behandlung bedroht sind, verbietet. Der EUROSUR-Verordnungsentwurf ist zu diesem Punkt beunruhigend still, obwohl die Europäische Kommission und FRONTEX argumentieren, ein ausdrückliches Ziel von EUROSUR sei die Rettung von Menschen aus Seenot – ein Ziel das stark im internationalen Recht verankert ist. In den Augen vieler Beobachter wird die Rechtmäßigkeit von EUROSUR in der Praxis davon abhängen, welche Priorität FRONTEX und die Mitgliedstaaten Such- und Rettungsaktionen und dem Recht auf Asyl einerseits und Überwachungs- und Abfangeinsätzen sowie so genannten „Push-back“-Aktionen andererseits einräumen. Auch wenn der Verordnungsvorschlag noch um einige Sicherheitsvorkehrungen ergänzt werden sollte, dürften diese Fragen im Legislativvorschlag weitestgehend fehlen. Es ist jedoch unumgänglich, die stillschweigende Ausweitung der Aufgaben und Befugnisse der Agentur FRONTEX, die in der EUROSUR-Verordnung vorgesehen ist, durch stärkere demokratische Kontrollen und Maßnahmen zu begleiten, um die Einhaltung internationalen Rechts zu gewährleisten. Dazu gehören strengere Regeln für die Zusammenarbeit mit Drittländern und deren Behörden, klarere Vorgaben für gemeinsame Einsätze und eine eindeutige Verpflichtung der EU zum Grundsatz der Nichtzurückweisung.

Auch die Pläne zu EES und RTP sind in einem weiteren politischen Zusammenhang zu sehen. In der Europäischen Union gibt es bereits drei riesige Einreisedatenbanken: das Schengener Informationssystem (SIS), mit dem „illegale“ Ausländer/-innen und Personen, die eine Gefahr für die Sicherheit der Mitgliedstaaten darstellen, erfasst und abgeschoben werden, EURODAC, in dem die Fingerabdrücke aller Asylsuchenden gespeichert werden und das Visa-Informationssystem (VIS), zu

dem eine der strengsten Visumpflichten der Welt gehört. Durch die Aufnahme „biometrischer Merkmale“ (Fingerabdrücke) in die zweite Generation der Systeme SIS und VIS, die sich ein biometrisches Abgleichsystem teilen, entsteht eine der größten Datenbanken für Fingerabdrücke weltweit. Das geplante EES würde die bestehenden Systeme ergänzen, Identität und Bewegungen von vielen Millionen Drittstaatenangehörigen erfassen, die derzeit keinem Visumzwang unterliegen, und automatisch potentielle Überzieher/-innen melden. So wie EUROSUR für einen Paradigmenwechsel in der Kontrolle der Hochsee steht, symbolisieren die Vorschläge zu EES und RTP den „nächsten Schritt“ bei der Einführung eines europaweiten biometrischen Zuwanderungssystems. Die Vorschläge scheinen uns eher das Produkt dieser politischen und wirtschaftlichen Bewegung zu sein als die rationale und kostengünstige Lösung einer gefühlten Zuwanderungskrise. Das Registrierungsprogramm für Reisende ist dazu gedacht, die Unannehmlichkeiten der verschärften Grenzkontrollen auszugleichen, dürfte aber in der Praxis nur wenigen vorab überprüften Geschäftsreisenden zur Verfügung stehen.

Außerdem sollten die Vorschläge angesichts der aktuellen Finanzkrise und der Folgen der Sparpolitik neu überdacht werden. Nach Schätzungen der Europäischen Kommission könnten sich die Kosten für die drei Systeme auf mindestens 1,5 Mrd. Euro belaufen. Das ist eine gewaltige Investition in IT-Großsysteme, über deren Erforderlichkeit – und Wirksamkeit – ernsthafte Zweifel bestehen.

5.1 EUROSUR

Das geplante Europäische Grenzüberwachungssystem ist ein ehrgeiziges und teures Projekt mit schwerwiegenden Auswirkungen auf die Grundrechte und die Entwicklung der Migrations- und Flüchtlingspolitik der Union im Allgemeinen. Vergleichbare Systeme, wie das Schengener Informationssystem und das EUROPOL-Informationssystem wurden auf der Grundlage von Primärrecht (Einführung) und Sekundärrecht (Umsetzung) entwickelt, das zumindest in gewissem Umfang im Europäischen Parlament, den nationalen Parlamenten und der Zivilgesellschaft diskutiert wurde. Bedenklicherweise wurde dieses Verfahren im Falle von EUROSUR durch einen technokratischen Prozess ersetzt, der es ermöglicht hat, das System schon zu entwickeln und durch umfangreiche öffentliche Finanzierung zu fördern, bevor nun endlich die Legislativvorschläge auf dem Tisch liegen.

Da der EUROSUR-Fahrplan von 2008 bereits umgesetzt wurde, bevor eine ordnungsgemäße Debatte und formelle Beratungsverfahren stattfinden konnten, gibt es nun kaum mehr die Möglichkeit, die Erforderlichkeit und Verhältnismäßigkeit der geplanten Systeme angesichts der zu erwartenden Kosten und möglichen Auswirkungen auf die Grundrechte zu diskutieren. Nach einer fünfjährigen Entwicklungsphase will die Europäische Kommission in nur einem Jahr (2013) den Rechtsrahmen für das EUROSUR-System verabschieden und das System (in einer Beta-Version) in Betrieb nehmen, was das Europäische Parlament praktisch vor vollendete Tatsachen stellt. Obwohl vom Parlament erwartet wird, den Vorschlag mit ein paar kosmetischen Korrekturen zu verabschieden, hat es doch die Möglichkeit, einige wichtige Sicherheitsvorkehrungen einzubauen. Außerdem muss das Parlament dafür sorgen, dass bei künftigen Initiativen, wie dem gemeinsamen Informationsraum für die Seeraumüberwachung der Europäischen Union, EES und RTP zuerst die rechtlichen und finanziellen Rahmenbedingungen festgelegt werden, bevor mit der Entwicklung der geplanten Systeme begonnen wird.

Wie bereits erwähnt, liegt die Rechtfertigung für EUROSUR in seiner Fähigkeit, „illegale Einwanderung“ zu bekämpfen, die Sicherheit Europas zu verbessern und Menschen aus Seenot zu retten. Diese Behauptungen sind mit Vorsicht zu genießen. Zum einen hängen sie von der noch unbewiesenen Kompatibilität neuer Technologien ab, zum anderen enthält der EUROSUR-Vorschlag keine Garantien dafür, dass Such- und Rettungseinsätze Vorrang haben. Angenommen die Technologie funktioniert, kann EUROSUR eindeutig dabei helfen, mehr Menschen in „Sicherheit“ zu bringen. Es gibt gewichtige Argumente dafür, umfangreiche finanzielle und personelle Ressourcen zur Rettung von Menschenleben im Mittelmeer einzusetzen. Allerdings wird an keiner Stelle des EUROSUR-Verordnungsvorschlags und der zahlreichen Folgenabschätzungen, Studien und Forschungs- und Entwicklungsprojekte konkret festgelegt, wie dies erreicht werden oder was mit den „Geretteten“ geschehen soll. An Bord der Boote, die FRONTEX mit Hilfe des Systems EUROSUR orten möchte, befinden sich normalerweise irreguläre Migrant/-innen und Personen, die internationalen Schutz benötigen. Es gibt jedoch keine Aussage zu der Frage, ob Asylanträge bearbeitet werden müssen. Wenn die Agentur FRONTEX und die Europäische Kommission es mit dem angeblichen Zweck von EUROSUR, der Rettung von Menschen aus Seenot, ernst meinen, muss der Verordnungsentwurf so geändert werden, dass Such- und Rettungseinsätze Vorrang haben und mit den Verpflichtungen des Flüchtlingsrechts und der Menschenrechtsnormen übereinstimmen. Dazu muss der Vorschlag zumindest das Verfahren festlegen, in dem EUROSUR Informationen oder Warnmeldungen an die Rettungsleitstellen des für den jeweiligen Such- und Rettungsbereich zuständigen Landes übermittelt. Außerdem muss der Agentur und den Mitgliedstaaten klar gemacht werden, dass sie Abfangeinsätze auf hoher See, mit denen Migrant/-innen daran gehindert werden, die europäischen Grenzen zu erreichen, nicht als Such- und Rettungseinsätze ausgeben dürfen. Letztere müssen eindeutig Vorrang haben. Außerdem müssen sich das Europäische Patrouillennetz, regionale Kooperationsnetze wie SEAHORSE und alle Drittstaaten, die zur Teilnahme an EUROSUR aufgefordert werden, verpflichten, die Bestimmungen des internationalen Übereinkommens zum Schutz des menschlichen Lebens auf See (SOLAS-Übereinkommen) und das Flüchtlingsrecht zu achten.

Ähnliche Bedenken gibt es zur technischen Durchführbarkeit des Vorschlags. Trotz der hochtechnologischen Behauptungen von „Ununterbrochener Überwachung“, „Lagebildern“ und „Grenzvorbereich-Informationen“ wurde das EUROSUR-System noch keiner ordnungsgemäßen technischen Risikobewertung unterzogen. EUROSUR hängt von der Einführung zahlreicher neuer Technologien und der Verknüpfung von 24 verschiedenen nationalen Koordinierungszentren und Überwachungssystemen ab – bilateral und über FRONTEX. Diese Entwicklung wird extrem komplex und extrem teuer. Dennoch sind die einzigen Akteure, die gefragt wurden, ob sie dies für durchführbar halten, die Agentur FRONTEX und die Unternehmen, die die entsprechenden Technologien verkaufen. Es ist kein logischer oder vertretbarer Grund erkennbar, warum das Verfahren zur Einrichtung von EUROSUR so übereilt vorangetrieben wird und Stellen wie die neue Europäische Agentur für IT-Großsysteme von dem Verfahren ausgeschlossen werden. Im Gegenteil sollte das vorgeschlagene EUROSUR-System und die Erfolgsaussichten der vielen Erkennungs- und Kommunikationstechnologien nun dank der zahlreichen Forschungs- und Entwicklungsprojekte, die von der Europäischen Kommission finanziert wurden, ausführlicher bewertet werden, bevor weitere EU-Mittel veranschlagt werden.

In der aktuellen Fassung scheint der Rechts- und Finanzrahmen für EUROSUR ein Freibrief für die Agentur FRONTEX und die Europäische Kommission zu sein, mit dem sie weiterhin so lange Forschung und Entwicklung aus dem Unionshaushalt finanzieren, bis sie ein funktionierendes System gefunden haben. EUROSUR selbst wurde nie ordnungsgemäß durchkalkuliert und die Schätzwerte der Europäischen Union halten, wie in Abb. 9 dargestellt, nicht einmal der oberflächlichen Überprüfung stand, die dieser Bericht leisten kann. Die Finanzierung von EUROSUR als unterschiedliche mehrjährige Haushaltslinien, deren jährliche Finanzierungsprioritäten die Europäische Kommission und FRONTEX relativ frei bestimmen können, ist ganz offensichtlich ein Rezept für finanzielle Exzesse. Angesichts der bisherigen Ausgaben und der beispielhaften Haushalte des Fonds für innere Sicherheit, könnte EUROSUR die von der Kommission geschätzten Kosten leicht um das zwei- bis dreifache übersteigen (siehe Abb. 9). Wenn die Legislativvorschläge für EUROSUR, Horizont 2020 und den Fonds für innere Sicherheit nicht um eine Ausgabendeckelung ergänzt werden, ist das Parlament praktisch machtlos gegen derartige Mehrkosten. Außerdem sollte das Parlament klare Regelungen dazu fordern, inwiefern der EUROSUR-Legislativvorschlag die Beschaffung von „Drohnen“ und anderen gemeinsamen Überwachungsinstrumenten durch FRONTEX mit EU-Mitteln vorsieht, und dafür sorgen, dass diese der demokratischen Debatte und angemessenen Kontrollen hinsichtlich der öffentlichen Sicherheit und zivilrechtlichen Haftung unterliegen.

Das Fehlen eines einheitlichen Verfahrens zur finanziellen Rechenschaftspflicht, das über die regelmäßigen Berichte hinausgeht, die FRONTEX und die Europäische Kommission ab Oktober 2015 vorlegen müssen, ist ebenfalls äußerst problematisch. Solange keine präzisen Berichte darüber vorliegen, was aus dem Budget von FRONTEX und den verschiedenen Haushaltslinien der EU für EUROSUR ausgegeben wird, ist es schon extrem schwierig zu überprüfen, wie hoch die Kosten für das Projekt bisher waren. Und der Ausschluss der Europäischen Agentur für IT-Großsystems hat die allgemeinen Aussichten für eine bessere Rechenschaftspflicht bei der Entwicklung von EUROSUR weiter stark verschlechtert. Da EUROSUR vor allem gegen „illegale Migration“ auf See gerichtet ist, erscheint es außerdem nicht erforderlich, die nördlichen Mitgliedstaaten bzw. die Mitgliedstaaten ohne Seegrenzen von Anfang an in das System EUROSUR zu integrieren. Angesicht der angespannten Haushaltslage wäre es sicherlich empfehlenswert, EUROSUR langsamer zu entwickeln: anfangs als Kommunikationsnetz der zehn Mitgliedstaaten, die zum bereits bestehenden Europäischen Patrouillennetz gehören, wobei neuen Technologien und Mitgliedstaaten in das Netz aufgenommen werden, falls und wenn (i) eine klare Notwendigkeit dazu besteht und (ii) deren Aufnahme gerechtfertigt ist.

In der EUROSUR-Verordnung fehlen angemessene Sicherheitsvorkehrungen zum Datenschutz. Obwohl EUROSUR personenbezogene oder biometrischen Daten nur in geringem Umfang erfassen wird und auch nicht zur Einrichtung einer zentralisierten Datenbank zur Datenspeicherung führt, könnten in verschiedenen „Schichten“ der Lagebilder personenbezogene Daten verarbeitet werden. FRONTEX kann die Daten neuer Überwachungssysteme, wie z. B. Drohnen, im Rahmen der „gemeinsamen Anwendung von Überwachungsinstrumenten“ nutzen, um den nationalen Koordinierungszentren und der Agentur Überwachungsinformationen über die Außengrenzen und den Grenzvorbereich zur Verfügung zu stellen. Außerdem wird EUROSUR die Grenzkontroll-Funktion des gemeinsamen Informationsraums der Union übernehmen und in dieser Rolle Daten mit zahlreichen Akteuren austauschen, zu denen auch Verteidigungskräfte gehören. All diese

Einsatzgebiete lassen viele Fragen bezüglich des Schutzes von Privatsphäre und personenbezogenen Daten offen, die im aktuellen Verordnungsvorschlag nicht ausreichend behandelt werden.

Der Verordnung muss eine besondere Bestimmung hinzugefügt werden, die ausdrücklich und erschöpfend die Bedingungen aufzählt, unter denen personenbezogene Daten im EUROSUR-System verarbeitet und mit externen Stellen und Behörden ausgetauscht werden dürfen. Da der Datenaustausch zwischen EUROSUR und „benachbarten Drittländern" auf der Grundlage bilateraler oder multilateraler Vereinbarungen zwischen einem oder mehreren Mitgliedstaaten und einem oder mehreren Drittländern erfolgen würde, ist es auch unerlässlich, eine Meldepflicht für diese Art von Datenaustausch einzuführen, damit die einzelstaatlichen Aufsichtsorgane die Weitergabe von Daten an Drittländer kontrollieren und sicherstellen können, dass dieser Datenaustausch nicht gegen Grundrechte verstößt. Die EUROSUR-Verordnung sollte außerdem ausdrücklich ein stufenweise aufgebautes Kontrollsystem vorsehen, bei dem die nationalen Datenschutzbeauftragten die Verarbeitung personenbezogener Daten durch die nationalen Koordinierungszentren überwachen und der europäische Datenschutzbeauftragte die Verarbeitung personenbezogener Daten durch FRONTEX kontrolliert. Derzeit ist nicht klar, ob der Verordnungsentwurf eine derartige stufenweise aufgebaute Kontrolle vorsieht.

Schließlich schlagen wir vor, die Umsetzung des Europäischen Programms für Sicherheitsforschung einer stärkeren demokratischen Kontrolle zu unterwerfen, um zu verhindern, dass Privatunternehmen die Forschungsagenda bestimmen und Verteidigungs- und Sicherheitsunternehmen die jährlichen Projektausschreibungen beeinflussen. Dadurch könnte sichergestellt werden, dass mit EU-Mitteln finanzierte Forschung sich schon von vornherein an den Grundrechten orientiert, wirklich Bedürfnisse erfüllt und wirtschaftlich sinnvoll ist.

5.2 „Intelligente Grenzen"

Sowohl EES als auch RTP sehen die Schaffung einer zentralisierten europäischen Datenbank vor, die möglicherweise höchst sensible biometrische Daten, wie Fingerabdrücke und Gesichtsbilder, von Millionen Menschen enthalten wird. Alle Drittstaatenangehörigen, die in den Schengenraum einreisen möchten, hätten keine andere Wahl, als der Verarbeitung ihrer personenbezogenen Daten zuzustimmen. Für eine derart umfassende Datenspeicherung müssen offensichtlich überzeugende Gründe der öffentlichen Sicherheit oder öffentlichen Ordnung angeführt werden, die zeigen, dass es sich um eine verhältnismäßige politische Reaktion handelt. Bisher wurde nicht nachgewiesen, dass EES oder RTP eine dringende soziale Notwendigkeit erfüllen.

Das EES wird grundsätzlich damit gerechtfertigt, das System würde die Ausweisung von Personen erleichtern, die ihre genehmigte Aufenthaltsdauer überschritten haben, und so der Einwanderungspolitik der Union mehr Glaubwürdigkeit verleihen. Diese Argumentation weist jedoch einige Schwächen auf. Es gibt viele rechtmäßige Gründe für die Überziehung der genehmigten Aufenthaltsdauer und viele Ausnahmen im Schengener Grenzkodex bezüglich der Registrierung von Ein- und Ausreisen. Daher dürfte eine EES-Warnmeldung allein kaum eine Abschiebung oder Ausweisung begründen. Eine Überschreitungswarnmeldung kann höchstens die Vermutung eines illegalen Aufenthalts anzeigen. Daher müssen klare Regeln für die Behandlung von Personen eingeführt werden, die als Überzieher/-innen gemeldet werden, damit gewährleistet ist, dass die

Union ihre Menschenrechtsverpflichtungen erfüllt. Um festzustellen, ob Personen sich rechtmäßig in der EU aufhalten, muss ein administratives Verfahren durchgeführt werden, in dessen Verlauf der Reisende die Umstände seiner Fristüberschreitung erklären kann. Außerdem ist es nach derzeitiger Rechtslage nicht möglich, eine EES-Warnmeldung in das SIS bzw. SIS II-System einzuspeisen, das nur die Aufnahme von Ausweisungsbescheiden eines Gerichts oder einer anderen zuständigen Behörde erlaubt. Da also ein „Treffer" im EES keine unmittelbaren Folgen für Überzieher/-innen hat, ist äußerst fraglich, ob das System wirklich zu effizienteren Rückführungen beiträgt. Jeder Versuch, EES-Warnmeldungen automatisch mit SIS bzw. SIS II zu verknüpfen, würde höchstwahrscheinlich zur Kontrolle einer inakzeptabel großen Anzahl absolut legaler Reisender führen. Außerdem darf man nicht vergessen, dass die Grenzposten bereits überprüfen, ob ausreisende Visuminhaber ihre genehmigte Aufenthaltsdauer überschritten haben. Die Einführung von halbautomatischen Kontrollen würde ihnen diese Aufgabe nicht abnehmen, sondern höchstens erleichtern.

Das EES wird sicher auch zu längeren Wartezeiten für Drittstaatenangehörige führen, die in den Schengenraum einreisen möchten. Bei Drittstaatenangehörigen, die ein Visum für die Einreise benötigen, werden bei der Einreise bereits biometrische Daten erfasst. Personen auf den so genannten weißen Listen, die kein Visum benötigen, sind von der Erfassungspflicht befreit. Wenn man von den Grenzkontrollzahlen ausgeht, die bei einer weiträumigen Überwachungsübung im Jahr 2009 erhoben wurden, könnte dies dazu führen, dass von weiteren 57 Millionen Drittstaatenangehörigen, die auf einer „weißen Liste" stehen, Fingerabdrücke erfasst werden müssten. Laut Folgenabschätzung für das VIS aus dem Jahr 2004 dauern die Formalitäten bei der Einreise in die USA durchschnittlich 15 Sekunden länger, seit in den Vereinigten Staaten biometrische Daten für das Programm US VISIT erfasst werden. Auch wenn die EU diese Zielvorgabe bei den 57 Millionen Drittstaatenangehörigen erreichen könnte, würde an den Grenzen der Union dadurch jährlich eine zusätzliche Wartezeit von 27 Jahren entstehen. Auch müssten Regeln für den Umgang mit irrtümlichen Warnmeldungen, Personen, bei denen bestimmte biometrische Merkmale nicht erfasst werden können, und zahlreiche weitere Eventualitäten festgelegt werden.

Die Kommission möchte diese zusätzlichen Einschränkungen des grenzüberschreitenden Reiseverkehrs durch die Einführung eines Registrierungsprogramms für Reisende abmildern, mit dessen Hilfe registrierte Reisende wesentlich schneller durch die Grenzkontrollen gelangen als ihre nicht registrierten Mitreisenden. Nach Schätzungen der Kommission könnten pro Jahr 4-5 Millionen Reisende das RTP nutzen, obwohl jährlich bis zu 100 Millionen Drittstaatenangehörige in den Schengenraum einreisen. Die Wartezeiten an den Gates für registrierte Reisende sind derzeit vor allem deshalb kürzer, weil nur relativ wenige Menschen an derartigen Programmen teilnehmen (die normalerweise eine Jahresgebühr von rund 125 Euro erheben). Daher sind ernsthafte Zweifel angebracht, ob diese Kontrollgates den Druck auf die Grenzen des Schengenraums senken oder für die große Mehrzahl das Reisen erleichtern können.

Nach Angaben der Kommission könnte die Entwicklung der zentralen Elemente von EES und RTP Kosten in Höhe von 450 Mio. Euro verursachen und die jährlichen Betriebskosten in den ersten fünf Jahren Kosten in Höhe von 190 Mio. Euro. Die Kommission hat 1,1 Mrd. Euro aus dem geplanten Fonds für innere Sicherheit (ISF) 2014-2020 für Entwicklung und Einführung dieser Systeme veranschlagt. Da aber nicht klar ist, ob diese Schätzwerte die vollständige Umsetzung des Visa-

Informationssystems in allen Schengenstaaten voraussetzen, könnten die tatsächlichen Zahlen wesentlich höher ausfallen. Wenn man bedenkt, dass das VIS noch nicht voll einsatzfähig ist und die Europäische Kommission und ihre Technologiepartner auch das SIS II noch nicht erfolgreich einführen konnten, scheint es geradezu grotesk, ein weiteres IT-Großprojekt anzustoßen, bevor auch nur die Funktionsfähigkeit eines der beiden anderen Systeme angemessen bewertet wurde. Anstatt ein teures zentralisiertes Registrierungsprogramm für Reisende aufzubauen, wäre es zu diesem Zeitpunkt sicherlich besser, sich auf die Kompatibilität zwischen den in den Mitgliedstaaten bereits bestehende lokalen oder nationalen Programmen zu konzentrieren und dann zu analysieren, ob ein europaweites System überhaupt erforderlich ist.

6 Empfehlungen

Wir wurden gebeten, Sicherheitsklauseln zu empfehlen, die in den EUROSUR-Verordnungsvorschlag und die künftigen Rechtsvorschriften zur Schaffung von EES und RTP aufgenommen werden können. Wie oben ausgeführt, hegen wir ernste Zweifel bezüglich des aktuellen EUROSUR-Legislativvorschlags und sind nicht von der Notwendigkeit des EES und RTP überzeugt. Wir haben auch starke Vorbehalte was die aktuelle Entwicklung der Grenzschutzpolitik der Union angeht und die Rolle, die eine immer weitergehende Überwachung in diesem Zusammenhang spielt. Daher sprechen wir zunächst einige allgemeine Empfehlungen zur Migrationspolitik der Europäischen Union aus und behandeln danach den Schutz der Grundrechte und eine stärkere demokratische Kontrolle des EUROSUR-Legislativvorschlags und der kommenden Vorschläge zu EES und RTP.

6.1 Grundsätze der Migrationspolitik der Europäischen Union

- Totale Überwachung und die Behandlung aller Reisenden als potentielle Verdächtige bilden keine rechtmäßigen, erforderlichen, wirksamen oder wünschenswerten Eckpfeiler für die Migrationspolitik der Europäischen Union. Die EU sollte diese politischen Initiativen aufgeben und durch Politikinstrumente ersetzen, die Überwachung auf ein absolut notwendiges Minimum beschränken, die Grundrechte achten sowie angemessene und erreichbare Politikinstrumente zur Einwanderungskontrolle nutzen.

- Die Externalisierung der europäischen Einwanderungskontrollen und der Einsatz von Entwicklungshilfe und technischer Unterstützung zur Schaffung von „Pufferzonen“, in denen Migrant/-innen und Flüchtlinge für die Sicherheitsbedürfnisse der EU durch Drittstaaten kontrolliert und festgehalten werden, ist nicht mit den politischen Zielen der Union im Bereich der Entwicklung und der Menschrechte vereinbar. Die EU sollte sich für ihre Beziehungen mit Drittländern im Bereich der Migration eine neue Agenda geben, in der die Sicherheit von Menschen im Mittelpunkt steht.

- Die immer stärkere Rolle der Sicherheits- und Verteidigungsbranche bei der Entwicklung und Umsetzung der Grenzschutzpolitik der Union (die mit dem Ausschluss von Zivilgesellschaft und Menschenrechtsorganisationen einhergeht) muss zu ernsten Interessenkonflikten führen. Die EU sollte ihre enge Partnerschaft mit der Sicherheitsbranche vor dem Hintergrund ihrer in den Verträgen festgelegten Verpflichtungen neu überdenken, damit gewährleistet ist, dass diese Risiken weitestgehend ausgeschlossen sind und eine ausgewogene Mischung von Interessengruppen zur politischen Willensbildung beiträgt.

6.2 EUROSUR

- Aufnahme von Bestimmungen in den EUROSUR-Verordnungsvorschlag, die die Nutzer von EUROSUR zu Such- und Rettungseinsätzen und zur Einhaltung von Flüchtlingsrecht und Menschenrechtsnormen verpflichten. Diese sollten eine klare Benennung der

Verpflichtungen gemäß dem SOLAS-Übereinkommen sowie eine deutliche Unterscheidung zwischen „Such- und Rettungs-„ und „Überwachungs- und Abfang“-Einsätzen umfassen.

- Aufnahme einer besonderen Bestimmung in den EUROSUR-Verordnungsvorschlag, die ausdrücklich und erschöpfend die Bedingungen aufzählt, unter denen personenbezogene Daten im EUROSUR-System verarbeitet werden dürfen, und an Dritte, d. h. auch an Verteidigungskräfte, weitergegeben werden dürfen.

- Aufnahme einer Bestimmung in den EUROSUR-Verordnungsvorschlag, die die NKZ und FRONTEX zur Führung eines Protokolls verpflichtet, in dem alle Transaktionen mit Drittländern verzeichnet werden, um die nationalen und/oder europäischen Aufsichtsorgane in die Lage zu versetzen, die Übermittlung von Daten an Drittstaaten zu kontrollieren. Diese Bestimmung sollte so detailliert sein, dass mit ihr die Einhaltung des im Legislativvorschlag enthaltenen Verbots sichergestellt ist, Informationen mit einem Drittstaat auszutauschen, der die betreffenden Informationen verwenden könnte, um Personen oder Gruppen ausfindig zu machen, die ernsthaft gefährdet sind, Opfer von Folter, einer unmenschlichen oder erniedrigenden Behandlung oder Strafe oder einer anderen Verletzung der Grundrechte zu werden.

- Aufnahme einer Bestimmung in den EUROSUR-Verordnungsvorschlag, die ein System der stufenweisen Kontrolle vorschreibt, bei dem die Datenschutzorgane der Mitgliedstaaten die Verarbeitung personenbezogener Daten durch die nationalen Koordinierungszentren von EUROSUR kontrollieren und der Europäische Datenschutzbeauftragte die Verarbeitung personenbezogener Daten durch die Agentur FRONTEX.

- Aufnahme weiterer Bestimmungen zur finanziellen Rechenschaftspflicht, die FRONTEX und die Europäische Kommission verpflichten, einen Jahresbericht vorzulegen, der alle Ausgaben für Entwicklungsprojekte mit Bezug zu EUROSUR aller Haushaltslinien der EU aufführt, einschließlich Außengrenzenfonds, Fonds für innere Sicherheit, FP7 und Horizont 2020 und Finanzierungsinstrument für die Entwicklungszusammenarbeit.

- In den Legislativvorschlag für das Programm Horizont 2020 sollte eine Bestimmung aufgenommen werden, die dem Europäischen Parlament eine Kontrolle der jährlichen Projektausschreibungen ermöglicht. Im Bereich der Sicherheits- und Weltraumforschung sollte das Kontrollverfahren gewährleisten, dass mit EU-Mitteln geförderte Forschungsprojekte von vorne herein die Grundrechte berücksichtigen, ein nachweisbares Sicherheitsbedürfnis erfüllen und wirtschaftlich sinnvoll sind.

- Beauftragung des Referats Bewertung wissenschaftlicher und technologischer Optionen des Europäischen Parlaments (STOA) mit der Durchführung einer technologischen Risikobewertung, der Kontrolle der mit EU-Mitteln geförderten Forschung und Entwicklung und der Durchführung einer Datenschutz-Folgenabschätzung für EUROSUR.

- Das Europäische Parlament sollte die Agentur der Europäischen Union für Grundrechte mit der Erstellung eines Gutachterberichts beauftragen, der überprüft, wie die Ressourcen der EU optimal für die Erhöhung der Sicherheit von Migrant/-innen und Flüchtlingen auf See unter gleichzeitiger Wahrung der Grundrechte eingesetzt werden können.

6.3 Einreise-/Ausreisesystem und Registrierungsprogramm für Reisende

- Jede künftige Rechtsvorschrift zum EES muss von der Voraussetzung ausgehen, dass eine „Überziehungsmeldung" nur die *Vermutung* eines illegalen Aufenthalts begründet. Nach Ausgabe der Warnmeldung, lässt sich nur in einem Verwaltungsverfahren bestimmen, ob sich die betreffende Person rechtmäßig auf dem Gebiet der Europäischen Union aufhält.

- Ein künftiges EES muss alle derzeit bestehende Ausnahmen im Schengener Grenzkodex (insbesondere in Anhang VI und VII) berücksichtigen, die bestimmte Personengruppen vom Zwang zu Einreise- oder Ausreisestempeln bei der Einreise oder Ausreise in den Schengenraum befreien.

- Ein künftiges EES sollte Situationen berücksichtigen, in denen Personen aus Gründen, für die sie nicht verantwortlich sind, bei der Ein- oder Ausreise nicht registriert wurden. Derartige Situationen dürfen nicht zur einer „Überziehungsmeldung" führen.

- Ein künftiges EES sollte auch Drittstaatenangehörigen die Einreise ermöglichen, die (körperlich) nicht in der Lage waren, sich in einem Programm zu registrieren, das biometrische Daten verwendet.

- Ein künftiges EES sollte strenge Sicherheitsvorkehrungen zum Datenschutz enthalten, zu denen auch ein Auskunftsrecht für Personen, die eine Registrierung im RTP beantragen, und für alle Drittstaatenangehörigen, deren Daten im EES verarbeitet werden, gehört. Dabei ist Auskunft über die folgenden Informationen zu erteilen:
    - Identität der für die Verarbeitung Verantwortlichen,
    - die Zwecke der Datenverarbeitung,
    - die Kategorien der Datenempfänger,
    - die Aufbewahrungsfrist der Daten,
    - ihr Auskunftsrecht bezüglich der über sie gespeicherte Daten einschließlich
        - das Recht, die Löschung von Daten zu verlangen, die unrichtig sind oder unrechtmäßig verarbeitet wurden,
        - das Recht auf Informationen über die Verfahren zur Ausübung dieser Rechte und die einzelstaatlichen Kontrollbehörden, die Beschwerden hinsichtlich des Schutzes personenbezogener Daten entgegennehmen.

- Ein künftiges RTP und EES muss die Antragsteller/-innen über die Beschwerdeverfahren informieren, mit denen sie gegen eine Ablehnung ihrer Registrierung im RTP oder eine Einstufung als Overstayer Beschwerde einlegen können. Beide Systeme müssen die Möglichkeit vorsehen, gegen diese Entscheidungen Beschwerde einzulegen oder deren

Überprüfung durch zuständige Gerichte oder Behörden zu erreichen, deren Mitglieder unparteiisch und in den Mitgliedstaaten, die „Überziehungswarnmeldungen“ ausgeben, unabhängig sind und die Angemessenheit und Rechtmäßigkeit der Maßnahme beurteilen.

- Die Notwendigkeit des Zugriffs von Strafverfolgungsbehörden muss gegebenenfalls in jedem Einzelfall nachgewiesen werden und zeigen, dass die Daten nicht oder nur unter großen Schwierigkeiten auf anderem Wege erhältlich sind, der keinen derartigen starken Eingriff bedeutet. Um eine Überprüfung dieses Grundsatzes zu ermöglichen, muss ein Protokoll eingeführt werden, das jeden Zugriff von Strafverfolgungsbehörden auf Daten des EES verzeichnet. Die Verwendung der im EES gespeicherten Daten muss ausdrücklich und restriktiv festgelegt werden, und die Festlegung muss über allgemeine Aussagen wie „für die Erfüllung ihrer Aufgaben erforderlich“ hinausgehen. In diesem Zusammenhang muss die Beziehung zwischen dem EES und den Systemen VIS und SIS bzw. SIS II im Legislativvorschlag genau beschrieben werden.

- Die Daten aller Drittstaatenangehörigen, die ordnungsgemäß in den Schengenraum ein- und wieder ausgereist sind, müssen unmittelbar nach Bestätigung der Ausreise gelöscht werden.

Die Autoren

Dr. Ben Hayes ist Projektdirektor der in London ansässigen Bürgerrechtsorganisation Statewatch, für die er seit 1996 tätig ist. Seine Spezialgebiete sind die Justiz- und Innenpolitik der Europäischen Union, Polizeiarbeit, Strafrecht, internationale Beziehungen und internationale Sicherheit. Er ist Fellow am Transnational Institute (TNI) mit Sitz in Amsterdam.

Mathias Vermeulen ist Forschungsstipendiat am European University Institute (EUI) in Florenz und wissenschaftliche Hilfskraft der Forschungsgruppe Recht, Wissenschaft, Technologie und Gesellschaft (LSTS) an der Vrije Universiteit Brüssel.