HEINRICH BÖLL STIFTUNG

The Greens | European Free Alliance
in the European Parliament

Borderline

The EU's New Border Surveillance Initiatives

Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals

A study by the Heinrich Böll Foundation

Written by
Dr. Ben Hayes
Mathias Vermeulen

June 2012

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

Ska Keller
Member of the European Parliament, Greens/EFA
European Parliament, Rue Wiertz 60, B-1047 Brussels
phone: +32 (0)2 28 45379
email: franziska.keller@europarl.europa.eu

Contents

Abbreviations 3
Preface 4
Executive Summary 7
1 Introduction 11
2 Towards “smart borders” in the European Union? 12
2.1 EUROSUR: European External Border Surveillance System 13
2.1.1 The EUROSUR roadmap 17
2.1.2 The draft EUROSUR Regulation 18
2.1.3 Beyond border control: integrated maritime surveillance 21
2.2 The EU “smart borders” initiative 26
2.2.1 Entry-exit system 28
2.2.2 EES relationship to existing EU systems: VIS and SIS II 30
2.2.3 Registered Traveller Programme 32
3 The fundamental rights impact of the EUROSUR and EU “smart border” initiatives 35
3.1 The right to privacy and the protection of personal data 36
3.1.1 EUROSUR 36
3.1.1.1 The need for safeguards 39
3.1.2 Smart borders 40
3.1.2.1 The need for safeguards 44
3.2 Interference with the right to asylum 45
3.2.1 EUROSUR 46
3.2.2 Entry-exit system 47
4 Cost, necessity, and effectiveness 49
4.1 Feasibility studies and cost estimates 49
4.1.1 EUROSUR 50
4.1.2 Entry-Exit System and Registered Traveller Programme 53
4.2 Border security and the European Security Research Programme 55
4.2.1 EU funded R&D projects supporting EUROSUR 58
4.2.2 Space-based border surveillance and the Common Information Sharing Environment 64
4.2.3 EU funded R&D projects supporting smart borders 66
4.3 Funding the implementation of EUROSUR and smart borders 67
4.3.1 The EU External Borders Fund 67
4.3.2 The Development Cooperation Instrument 68
4.3.3 The Internal Security Fund 69
4.4 The United States’ experience: SBI-net and US VISIT 70
5 Conclusions 73
5.1 EUROSUR 74
5.2 Smart borders 76
6 Recommendations 79

Authors 82

List of Figures and Boxes

Figure 1: the planned EUROSUR system 13
Figure 2: "Operational nodes" in the Common Pre-Frontier Intelligence Picture 21
Figure 3: EUROSUR and the Common Information Sharing Environment 22
Figure 4: "Policy options" for funding EUROSUR 52
Figure 5: Estimated EUROSUR costs: National Coordination Centres and FRONTEX 52
Figure 6: Estimated costs of the RTP and EES systems by the Commission 54
Figure 7: Achieving border security in the EU 58
Figure 8: Cost of establishing, upgrading, and maintaining NCCs 2011–2026 68
Figure 9: Questioning the EUROSUR cost estimates 70

Box 1: The EUROSUR roadmap 17
Box 2: EUROSUR – A system of systems 23
Box 3: The Visa Information System and the Schengen Information System/SIS II 31
Box 4: EU security research projects supporting EUROSUR 60
Box 5: GMES projects supporting EUROSUR 65

Abbreviations

AIS	Automatic Identification Systems
CISE	Common Information Sharing Environment
EBF	External Borders Fund
ECPN	European Coastal Patrol Network
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EES	Entry-Exit System
EMSA	European Maritime Safety Agency
ESRP	European Security Research Programme
EUROSUR	European External Border Surveillance System
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
FSC	FRONTEX Situation Centre
GMES	Global Monitoring for Environment and Security
ISF	Internal Security Fund
LRIT	Long Range Identification and Tracking
NCC	National Coordination Centre
RTP	Registered Traveller Programme
SBI-net	Secure Border Initiative
SIS	Schengen Information System
TCN	Third-country National
VIS	Visa Information System
VMS	Vessel Monitoring Systems
VDS	Vessel Detection System

Preface

The upheavals in North Africa have lead to a short-term rise of refugees to Europe, yet, demonstrably, there has been no wave of refugees heading for Europe. By far most refugees have found shelter in neighbouring Arab countries. Nevertheless, in June 2011, the EU's heads of state precipitately adopted EU Council Conclusions with far-reaching consequences, one that will result in new border policies "protecting" the Union against migration. In addition to new rules and the re-introduction of border controls within the Schengen Area, the heads of state also insisted on upgrading the EU's external borders using state-of-art surveillance technology, thus turning the EU into an electronic fortress.

The Conclusions passed by the representatives of EU governments aims to quickly put into place the European surveillance system EUROSUR. This is meant to enhance co-operation between Europe's border control agencies and promote the surveillance of the EU's external borders by FRONTEX, the Union's agency for the protection of its external borders, using state-of-the-art surveillance technologies. To achieve this, there are even plans to deploy unmanned aerial vehicles (UAVs) over the Mediterranean and the coasts of North Africa. Such high-tech missions have the aim to spot and stop refugee vessels even before they reach Europe's borders. A EUROSUR bill has been drafted and is presently being discussed in the European Council and in the European Parliament.

Member states also want to introduce so-called "smart borders" to achieve total control over all cross-border movements. Following the US model, the plan is to introduce a massive database that will store information, including fingerprints, of all non-EU citizens leaving or entering the Union. The aim is to identify so-called "over-stayers," that is, third-country nationals who have overstayed their permission to stay. In the United States, a similar system has been a failure and nationwide exit checks were never introduced. Still, the EU's heads of state and its government representatives persist – whatever the cost (the EU Commission estimates it will be up to €1.1 billion). Under pressure from member states, it is trying to introduce the smart borders bill during the summer of 2012.

EUROSUR and "smart borders" represent the EU's cynical response to the Arab Spring. Both are new forms of European border controls – new external border protection policies to shut down the influx of refugees and migrants (supplemented by internal controls within the Schengen Area); to achieve this, the home secretaries of some countries are even willing to accept an infringement of fundamental rights.

The present study by Ben Hayes and Mathias Vermeulen demonstrates that EUROSUR fosters EU policies that undermine the rights to asylum and protection. For some time, FRONTEX has been criticised for its "push back" operations during which refugee vessels are being intercepted and escorted back to their ports of origin. In February 2012, the European Court of Human Rights condemned Italy for carrying out such operations, arguing that Italian border guards had returned all refugees found on an intercepted vessel back to Libya – including those with a right to asylum and international protection. As envisioned by EUROSUR, the surveillance of the Mediterranean using

UAVs, satellites, and shipboard monitoring systems will make it much easier to spot such vessels. It is to be feared, that co-operation with third countries, especially in North Africa, as envisioned as part of EUROSUR, will lead to an increase of "push back" operations.

Nevertheless, the EU's announcement of EUROSUR sounds upbeat: The planned surveillance of the Mediterranean, we are being told, using UAVs, satellites, and shipboard monitoring systems, will aid in the rescue of refugees shipwrecked on the open seas. The present study reveals to what extent such statements cover up a lack of substance. Maritime rescue services are not part of EUROSUR and border guards do not share information with them, however vital this may be. Only just recently, the Council of Europe issued a report on the death of 63 migrants that starved and perished on an unseaworthy vessel, concluding that the key problem had not been to locate the vessel but ill-defined responsibilities within Europe. No one came to the aid of the refugees – and that in spite of the fact that the vessel's position had been known.

In reaction to the Arab Spring, EU member countries are not only promoting a total surveillance of the Mediterranean, they are also pushing for an electronic upgrading of border controls. This means that ordinary travellers, too, will come into the focus of border guards in what one may well call a data juggernaut. Through its "smart borders" programme the EU would create one of the world's largest biometric databases – not with the aim to fight terrorism or stem cross-border crime (even that would be a questionable endeavour), but solely in order to identify individuals that have overstayed their permission to stay.

One of the fundamental findings of the study is that the EU's new border regime would not only infringe fundamental rights, it would also, in spite of its questionable benefits, cost billions – and that against the background of pervasive budget cuts and austerity measures. Above all, this would profit Europe's defence contractors, as they would receive EU funding for "smart gates," UAVs, and other surveillance technologies. The technological upgrading of the EU's external borders will obviously open up new markets to European security and armament companies. What we witness is a convergence of business interests and the aims of political hardliners who view migration as a threat to the EU's homeland security.

The EU's new border control programmes not only represent a novel technological upgrade, they also show that the EU is unable to deal with migration and refugees. Of the 500,000 refugees fleeing the turmoil in North Africa, less than 5% ended up in Europe. Rather, the problem is that most refugees are concentrated in only a very few places. It is not that the EU is overtaxed by the problem; it is local structures on Lampedusa, in Greece's Evros region, and on Malta that have to bear the brunt of the burden. This can hardly be resolved by labelling migration as a novel threat and using military surveillance technology to seal borders. For years, instead of receiving refugees, the German government along with other EU countries has blocked a review of the Dublin Regulation in the European Council. For the foreseeable future, refugees and migrants are to remain in the countries that are their first point of entry into the Union.

Within the EU, the hostile stance against migrants has reached levels that threaten the rescue of shipwrecked refugees. During FRONTEX operations, shipwrecked refugees will not be brought to the nearest port – although this is what international law stipulates – instead they will be landed in a port of the member country that is in charge of the operation. This reflects a "nimby" attitude – not in my backyard. This is precisely the reason for the lack of responsibility in European maritime rescue

operations pointed out by the Council of Europe. As long as member states are unwilling to show more solidarity and greater humanity, EUROSUR will do nothing to change the status quo.

The way forward would be to introduce improved, Europe-wide standards for the granting of asylum. The relevant EU guidelines are presently under review, albeit with the proviso that the cost of new regulations may not exceed the cost of those in place – and that they may not cause a relative rise in the number of asylum requests. In a rather cynical move, the EU's heads of government introduced this proviso in exactly the same resolution that calls for the rapid introduction of new surveillance measures costing billions. Correspondingly, the budget of the European Asylum Support Office (EASO) is small – only a ninth what goes towards FRONTEX.

Unable to tackle the root of the problem, the member states are upgrading the Union's external borders. Such a highly parochial approach taken to a massive scale threatens some of the EU's fundamental values – under the pretence that one's own interests are at stake. Such an approach borders on the inhumane.

Berlin/Brussels, May 2012

Barbara Unmüßig
President Heinrich-Böll-Stiftung

Ska Keller
Member of the European Parliament

Executive Summary

The research paper "Borderline" examines two new EU border surveillance initiatives: the creation of a European External Border Surveillance System (EUROSUR) and the creation of the so-called "smart borders package", which includes the establishment of an Entry-Exit System (EES); and the creation of a Registered Traveller Programme (RTP). EUROSUR promises increased surveillance of the EU's sea and land borders using a vast array of new technologies, including drones (unmanned aerial vehicles), off-shore sensors, and satellite tracking systems. The EES would record the movement of people into and out of the Schengen area and extend biometric ID checks to all non-EU nationals (including those not currently subject to EU visa requirements) with the aim of helping border guards identify "overstayers", i.e. individuals that have overstayed their legal permission to stay. Since such biometric checks at all borders will result in significantly longer waiting lines, the creation of the EES is linked to the establishment of a Registered Traveller Programme that would enable pre-vetted individuals who are deemed not to pose a security risk to cross borders much faster than their unregistered counterparts. This system would rely on the use of automated border gates, which are already installed in some European airports. EU policy-makers and the manufacturers of these gates hope that this will lead to the general roll-out of so-called smart borders across the EU.

The EU's 2008 proposals gained new momentum with the perceived "migration crisis" that accompanied the 'Arab Spring' of 2011, which resulted in the arrival of thousands of Tunisians in France. These proposals are now entering a decisive phase. The European Parliament and the Council have just started negotiating the legislative proposal for the EUROSUR system, and within months the Commission is expected to issue formal proposals for the establishment of an EES and RTP.

Taken together, the EUROSUR and smart borders package could cost in the order of €2 billion or more. They would result in the gathering of biometric data on millions of travellers, longer waiting lines at the EU's external borders, and the establishment of costly new border surveillance systems in the member states and at FRONTEX, the EU border agency. The European Commission has produced several impact assessments but, according to the report, these have failed to demonstrate a pressing social need for the new systems. The Commission's financial estimates have a wide margin of error. EU institutions have failed to take into account the insurmountable difficulties that the United States has faced in introducing comparable systems (US VISIT, which is still unable to record the exit of travellers from the United States; and SBINET, a border surveillance system along the Mexican border that was scrapped after technological problems and exploding costs). The authors call for a proper public debate about both the need for yet more expensive EU-wide databases and surveillance systems in an era of crippling austerity.

The report is also critical of the decision-making process. Whereas the decision to establish comparable EU systems such as EUROPOL and FRONTEX were at least discussed in the European and national parliaments, and by civil society, in the case of EUROSUR – and to a lesser extent the smart borders initiative – this method has been substituted for a technocratic process that has allowed for

the development of the system and substantial public expenditure to occur well in advance of the legislation now on the table. Following five years of technical development, the European Commission expects to adopt the legal framework and have the EUROSUR system up and running (albeit in beta form) in the same year (2013), presenting the European Parliament with an effective fait accomplit.

The EUROSUR system

The main purpose of EUROSUR is to improve the "situational awareness" and reaction capability of the member states and FRONTEX to prevent irregular migration and cross-border crime at the EU's external land and maritime borders. In practical terms, the proposed Regulation would extend the obligations on Schengen states to conducting comprehensive "24/7" surveillance of land and sea borders designated as high-risk – in terms of unauthorised migration – and mandate FRONTEX to carry out surveillance of the open seas beyond EU territory and the coasts and ports of northern Africa. Increased situational awareness of the high seas should force EU member states to take adequate steps to locate and rescue persons in distress at sea in accordance with the international law of the sea. The Commission has repeatedly stressed EUROSUR's future role in "protecting and saving lives of migrants", but nowhere in the proposed Regulation and numerous assessments, studies, and R&D projects is it defined how exactly this will be done, nor are there any procedures laid out for what should be done with the "rescued". In this context, and despite the humanitarian crisis in the Mediterranean among migrants and refugees bound for Europe, EUROSUR is more likely to be used alongside the long-standing European policy of preventing these people reaching EU territory (including so-called push back operations, where migrant boats are taken back to the state of departure) rather than as a genuine life-saving tool.

The EUROSUR system relies on a host of new surveillance technologies and the interlinking of 24 different national surveillance systems and coordination centers, bilaterally and through FRONTEX. Despite the high-tech claims, however, the planned EUROSUR system has not been subject to a proper technological risk assessment. The development of new technologies and the process of interlinking 24 different national surveillance systems and coordination centres – bilaterally and through FRONTEX – is both extremely complex and extremely costly, yet the only people who have been asked if they think it will work are FRONTEX and the companies selling the hardware and software. The European Commission estimates that EUROSUR will cost €338 million, but its methods do not stand up to scrutiny. Based on recent expenditure from the EU External Borders Fund, the framework research programme, and indicative budgets for the planned Internal Security Fund (which will support the implementation of the EU's Internal Security Strategy from 2014–2020), it appears that EUROSUR could easily end up costing two or three times more: as much as €874 million. Without a cap on what can be spent attached to the draft EUROSUR or Internal Security Fund legislation, the European Parliament will be powerless to prevent any cost overruns. There is no single mechanism for financial accountability beyond the periodic reports submitted by the Commission and FRONTEX, and since the project is being funded from various EU budget lines, it is already very difficult to monitor what has actually been spent.

In its legislative proposal, the European Commission argues that EUROSUR will only process personal data on an "exceptional" basis, with the result that minimal attention is being paid to privacy and data protection issues. The report argues that the use of drones and high-resolution cameras means

that much more personal data is likely to be collected and processed than is being claimed. Detailed data protection safeguards are needed, particularly since EUROSUR will form in the future a part of the EU's wider Common Information Sharing Environment (CISE), under which information may be shared with a whole range of third actors, including police agencies and defence forces. They also call for proper supervision of EUROSUR, with national data protection authorities checking the processing of personal data by the EUROSUR National Coordination Centres, and the processing of personal data by FRONTEX, subject to review by the European Data Protection Supervisor. EUROSUR also envisages the exchange of information with "neighbouring third countries" on the basis of bilateral or multilateral agreements with member states, but the draft legislation expressly precludes such exchanges where third countries could use this information to identify persons or groups who are at risk of being subjected to torture, inhuman and degrading treatment, or other fundamental rights violations. The authors argue that it will be impossible to uphold this provision without the logging of all such data exchanges and the establishment of a proper supervisory system.

Smart borders

Whereas the EUROSUR system focusses on unauthorised border crossings, the smart borders proposals are supposed to enhance checks on third-country nationals coming to the EU. Specifically, the proposed Entry-Exit System is supposed to identify and prevent overstayers, that is, persons who entered the EU legally with a valid travel document and/or visa, but who became "illegal migrants" when their legal entitlement to stay expired. According to the European Commission, this category of migrants constitutes the largest group of illegal immigrants in the EU. The EES would work by registering the time and place of entry and exit of third-country nationals in order to verify their exit and/or identify them if they have "overstayed". In this case, an alert would automatically be sent to relevant national authorities. The ESS plans the creation of a centralised European database that would include biometric data such as fingerprints and facial images from *all* third-country nationals entering the Schengen area. Data gathering on such a large scale is only legal and legitimate if there are compelling reasons that concern public safety or public order. The authors argue that the European Commission has failed to demonstrate the necessity of such data gathering.

The authors also argue that since there are many perfectly legal explanations as to why people overstay, an EES alert could never result in automatic sanctions. An alert could only constitute a *presumption* of illegal residence, and a follow-up (administrative) procedure would always be needed to determine whether a person has the right to stay legally in the EU or not. Thus, at best, the EES could only ever assist border guards in carrying out passenger checks; current claims that the EES as such would lead to an increase in the detection and return of "illegal immigrants" are unfounded. A further justification for the EES is that it would deliver better statistics on travel patterns and immigration routes, which is helpful for the EU's immigration policy. However, the gathering of such information could easily be done anonymously and in a much less expensive way. The gathering of a vast amount of personal data would clearly be a disproportional way to achieve that aim. Last but not least, there is also a lack of reliable evidence supporting the effectiveness and the efficiency of entry-exit systems at the national level and outside the EU.

An EES would also result in significantly increased waiting times for third-country nationals wanting to enter the Schengen area. Whereas third-country nationals subject to a visa requirement are

already required to provide biometric data on entry, those on the so-called "white list", who do not require an advance visa, are exempt from this requirement. Extrapolating from border-crossing statistics collected during a comprehensive monitoring exercise in 2009, this could result in the annual fingerprinting of an additional 57 million "white list" third-country nationals. An earlier impact assessment stated that, on average, 15 seconds were added to entry procedures in the United States when biometrics were introduced to its US VISIT programme. If the EU were able to achieve this target with regard to 57 million third-country nationals, this would still add the equivalent of 27 years of queuing time per year at EU borders. The Commission proposes to "offset" these additional constraints on cross-border travel by establishing a Registered Traveller Programme that enables pre-vetted individuals to cross borders much faster than their unregistered counterparts. However, the Commission has also estimated that only 4 to 5 million travellers per year might actually use an EU RTP, out of an estimated 100 million third-country nationals entering the Schengen area every year. While it would almost certainly make life easier for business travellers, an EU RTP would clearly not facilitate travel for the vast majority of travellers or relieve existing pressure at Schengen's external borders.

According to the European Commission, the cost of developing the central EES and RTP could be in the order of €400 million, plus annual operating costs of €190 million per year for the first five years. Despite the absence of any draft legislation, or even an agreement in principle on introducing smart borders in the EU, the Commission has already allocated €1.1 billion to the development of an EES and RTP from the proposed EU Internal Security Fund (2014–2020). The exploding costs and repeated delays in implementing the Schengen Information System II, which turned out to be at least five times as expensive as the initial estimates suggested, should give a strong warning signal to EU decision-makers that the decision to create these databases will have strong budgetary consequences at a time when strict austerity in other areas is creating a crisis of EU legitimacy. The authors of the study suggest that in any case it is unwise for the EU to even consider embarking on another large-scale IT system before the Visa Information System and Schengen Information System II have been successfully implemented. Assuming that the effectiveness of these two systems can be demonstrated, the Commission will still have a long way to go to demonstrate the need for smarter borders.

1 Introduction

The European Union's 500 million citizens inhabit a territory delineated by 7,400 km of land borders and 57,800 km of coastline ("maritime borders").[1] Some 300 million people – just under half of them non-EU citizens – are estimated to enter and leave the EU every year.[2] All but a tiny fraction do so completely legitimately. The arrival in Italy in early 2011 of around 25,000 Tunisians fleeing the turmoil that accompanied the so-called Arab Spring galvanised the European Union into action on three ambitious proposals to prevent unauthorised migration and residence.[3] These are (i) the creation of a European External Border Surveillance System (EUROSUR); (ii) the establishment of an Entry-Exit System (EES) to record the movement of people into and out of the Schengen area and help identify visa "overstayers"; and (iii) the establishment of a Registered Traveller Programme (RTP), under which third-country nationals (TCNs) who have been pre-vetted and deemed not to pose a security risk to the EU may benefit from faster entry into the Schengen area. Whether this represents a proportionate response to the relatively small number of refugees from North Africa who made their way to Europe during the recent political crises is something of a moot point;[4] the proposals were conceived long ago and have been under active consideration for more than four years, though it is only recently that the EU institutions have begun working on formal legislation.

We have been asked to assess whether the three aforementioned proposals comply with the EU Charter of Fundamental Rights and consider the merits of the proposals as compared to their likely cost, impact, and effectiveness. In attempting to address these questions, it is important to state that, whereas the legislation establishing EUROSUR was published in December 2011, the legislation establishing the EES and RTP, which was expected before the summer of 2012, will be delayed until later in the year, requiring us to examine earlier feasibility studies and interpret deliberations within the EU institutions. Another major challenge facing this study is that – under the terms of a "roadmap" issued by the European Commission in February 2008 – the development of EUROSUR is already well underway. This means it is not just a case of analysing the legislation but examining how the system is being implemented.

Section 2 of the report examines the development of the proposed EUROSUR System, Entry-Exit System, and Registered Traveller Programme. Section 3 assesses the compliance of the three proposed systems with the most relevant aspects of the EU Charter of Fundamental Rights. Section 4 examines the EU investments already made in EUROSUR and smart borders and the envisaged costs of implementing the proposals. Sections 5 and 6 provide conclusions and recommendations, respectively.

1 Council doc. 18666/11 ADD 1, p. 7.
2 "EU unveils plans for biometric border controls", EUobserver, 13 Feb. 2008, available at: http://euobserver.com/22/25650.
3 See EU Council Conclusions of 11 and 12 Apr. 2011, and 9 and 10 June 2011.
4 In June 2011 the UNHCR estimated that around 1 million people had fled to border countries, including Tunisia, Egypt, Algeria, Niger, and Chad. UNHCR, Update n° 29, "Humanitarian situation in Libya and the neigbouring countries", UNHCR 15 June 2011, available at: http://www.unhcr.org/4df9cde49.html.

2 Towards "smart borders" in the European Union?

The idea of "smart borders" gained credibility in the EU when the European Commission launched what came to be known as its "smart borders" initiative in February 2008. The proposals, which consisted of automated ID checks, border gates, increased pre-screening measures, and new databases, were accompanied by a second Communication containing a roadmap for the development of the European Border Surveillance System. "EUROSUR" envisages the use of coastal radar, satellite tracking systems, drones and autonomous targeting systems to detect small vessels bound for EU territory.

"This package designs a completely new way of controlling our borders," announced former Commissioner Franco Frattini of the 2008 package of proposals. The underlying assumption is that smart borders using new technologies both improve security – by (automatically) identifying threats and risks – while simultaneously increasing efficiency, by reducing human input or the time that travellers spend queuing to have their documents checked at passport control, for example. "We don't have an alternative", stated Commissioner Frattini. "It's because of terrorist threats, criminality, paedophile networks. We cannot have them using better technology than police."[5]

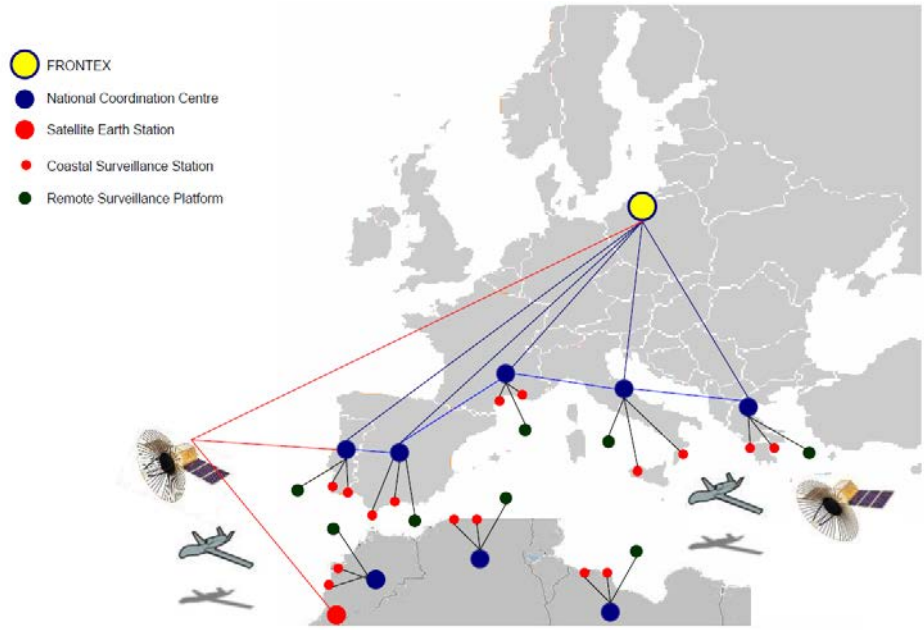
We are concerned from the outset that core assumptions about necessity and effectiveness have not been subject to rigorous, impartial scrutiny. We also have reservations about the sheer ambition and potential scope of the EUROSUR and smart borders proposals, which, taken together, would result in increased surveillance of EU border areas and the open waters beyond, and the gathering of personal data on millions of people. We also harbour serious doubts about the technical viability of the plans and the prospects of successfully aligning the information systems of numerous EU agencies with a vast array of national and international surveillance systems to the requisite operational standards across up to 30 different national-state immigration and border control systems.

A broader political issue is also at stake where 'smart borders' and high-tech responses to migration such as EUROSUR are concerned. The EU has increasingly resorted to technical solutions to perceived migration problems. These technical solutions are often presented as mere technical measures as if somehow separate from the EU's broader migration and border control policies (and thus less deserving of scrutiny or discussion) when they have moved ever closer to its core. We hope that this report contributes to a better understanding of the role that technology – and its suppliers – are now playing in shaping the EU's migration control policies and a much needed, broader debate about Europe's moral, ethical and legal responsibilities toward migrants and refugees.

5 "EU unveils plans for biometric border controls", EUobserver, 13 Feb. 2008, available at: http://euobserver.com/22/25650.

2.1 EUROSUR: European External Border Surveillance System

Figure 1: the planned EUROSUR system[6]



The development of the EUROSUR system should be seen as part of a long-term policy-making process. The entry into force of the Amsterdam Treaty in 1999 provided greater powers for the EU over national border controls, immigration, and asylum policies, and a new role for the European Commission in developing EU legislation. In terms of new EU policy initiatives, however, it was the member states who set an ambitious agenda with calls for an EU border police and a "global approach to migration"[7] – the former premised on the need to police the Mediterranean to prevent the arrival of irregular migrants and refugees, the latter premised on the externalisation and imposition of EU controls in states of origin and transit. The proposed EUROSUR system is essentially the product of this twin-track approach. The proposals discussed below should also be seen in relation to the European Commission's 2002 Communication on "integrated border management", which set out plans for a common "Schengen Borders Code", a practical handbook for border guards, and the creation of an "External Borders Fund" to strengthen controls in member states.[8]

Although not formally adopted until 2005, the EU's Global Approach to Migration dates back to 1997 and the arrival in Italy and Greece of thousands of Kurdish refugees from Iraq, who had travelled by sea from Turkey. This prompted the EU to draft a 46-point Action Plan to ensure that this kind of

6 GLOBE project presentation, available at: http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=5119.
7 Council doc. 13147/01.
8 COM (2002) 233 final. See also the Hague Programme 2004. The Borders Code was adopted in 2006 (Regulation 2006/562/EC) and €1.82 billion was allocated to the EU External Borders Fund 2007–2013.

"mass influx" did not recur.[9] The Iraq plan was followed by an Austrian Presidency strategy paper on migration, which suggested explicitly that a:

> [M]odel of concentric circles of migration policy could replace that of "fortress Europe" … the Schengen states currently lay down the most intensive control measures. Their neighbours should gradually be linked into a similar system … particularly with regard to visa control and readmission policies. A third circle of states (CIS area, Turkey, and North Africa) will then concentrate primarily on transit checks and combating facilitator networks, and a fourth circle (Middle East, China, black Africa) on eliminating push factors.[10]

The Austrian strategy paper was widely condemned by migrant and refugee organisations and disowned by the EU,[11] but the principles it contained were embodied in a 2002 EU Action Plan on illegal immigration.[12] The plan provided for EU funding for migration controls in countries of origin of migrants and refugees, including border management equipment and expertise, asylum-processing infrastructures, public registration structures (i.e. biometrics/databases), reception centres for illegal immigrants in transit countries, and "awareness-raising campaigns" for would be "illegal" émigrés. The Action Plan also called for the introduction of "migration management" clauses in EU agreements with third states, using the "levers" of aid-and-trade to ensure cooperation. The European Commission began funding "preparatory actions on cooperation with third countries in the field of migration" from the EC development budget (see section 4).[13]

In December 2005, following a special EU migration summit, the "global approach" was formally extended to include for the first time a "surveillance system covering the whole southern border of the EU and the Mediterranean Sea."[14] The European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), now formally up-and-running,[15] was requested to conduct the feasibility study. FRONTEX was also requested to conduct a second feasibility study on a "Mediterranean Coastal Patrols Network involving EU Member States and North African countries." FRONTEX produced the two feasibility studies with the assistance of experts from the member states and the EU's Joint Research Centre. The "MEDSEA" feasibility study on the Mediterranean Coastal Patrols Network was presented to the member states in July 2006 and subsequently published.[16] The "BORTEC" study on the EU Border Surveillance System was presented to the member states in January 2007, but it is classified as confidential and has not been published. The MEDSEA study recommended the creation of a permanent organisational structure to ensure "control and surveillance" of the entire length of the EU's southern maritime borders. Each participating member state would establish a National Coordination Centre (NCC) to work with FRONTEX, the other member states, and, where appropriate, third countries. In December 2006 the European Council invited FRONTEX to establish a

9 Council doc. 5573/98.
10 Council doc. 9809/98.
11 "EU Migration plan side-lined and resurrected", *Statewatch Bulletin* 8(6) (Nov.–Dec. 1998).
12 Council doc. 6621/1/02.
13 This programme evolved into the AENEAS budget line – a five-year, €250 million programme to improve migration controls in countries of origin and transit of migrants and refugees that began in 2004. Now called the Thematic Programme for Cooperation with Third countries in the Areas of Migration and Asylum, the programme has an annual budget of around €75 million.
14 EU Presidency conclusions of 15-16 Dec. 2005 [emphasis added]. See also COM (2005) 621 final.
15 Regulation 2007/2004/EC.
16 Council doc. 12049/06 EXT 1.

permanent European Coastal Patrol Network (ECPN) as soon as possible "to combat illegal immigration along the southern maritime borders."[17] The joint patrols of border guards, coastguards, and naval forces initially focussed on the Canary Islands and the area south of the Iberian Peninsula (led by Portugal and Spain), the northern Mediterranean (France), and the north Adriatic (Italy and Slovenia). Ten Mediterranean countries are now participating in the ECPN but there has been no external review of how it has been working to date.[18]

The BORTEC study analysed the coastal surveillance assets of seven member states[19] and recommended the establishment of what would later be called EUROSUR, based on increased coastal surveillance by the ECPN's National Coordination Centres and data sharing/fusion among them and with FRONTEX. It also recommended that "serious consideration" be given to the "further development of sensors, airborne and space borne unmanned means" to detect any vessel "of any size and material and an estimation of its speed and tack "in all weather conditions/sea state, day and night."[20] Surveillance would take place along all EU coastal waters up to a range of 30 nautical miles as well as in "wide sea bands close to third countries' coastal waters … Along the southern part of the Mediterranean starting from the Straits of Gibraltar up to Cyprus including the Aegean Sea as well as part of the Adriatic [and] Along the western coast of African countries."[21]

In addition to the Coastal Patrols Network and EUROSUR taken forward by FRONTEX, the European Commission is pursuing an "Integrated Maritime Policy for the EU" launched in October 2007. This policy implies that EUROSUR will ultimately be part of a "more interoperable surveillance system to bring together existing monitoring and tracking systems used for maritime safety and security, protection of the marine environment, fisheries control, control of external borders and other law enforcement activities."[22] A maritime surveillance network for the defence community is also being developed under the auspices of the European Defence Agency.[23] Both of these initiatives could have significant implications for the way the proposed EUROSUR system is developed and used in practice.

Finally, it is important to understand the potential role of EUROSUR in the context of legal and political debates about the legitimacy of joint EU migration control operations under the auspices of FRONTEX, or in the context of bilateral and regional state-to-state cooperation. Two considerations are important here. The first concerns so-called "push-back" operations, where persons bound for Europe are returned to their country of departure or a third state outside of the European Union and are thus denied the possibility of lodging an asylum application to a member state. In a landmark judgment in 2012, the European Court of Human Rights found that Italy had effectively presided over a "collective expulsion" that had exposed persons to an unacceptable risk of torture or ill-treatment when it intercepted a boat in the open seas and returned it to Libya in 2009, in breach of

17 European Council Conclusions, 14–15 Dec. 2006. See also EU Press Release on ECPN, MEMO/07/203, 24 May 2007.
18 The participating countries are Bulgaria, Cyprus, Spain, France, Greece, Italy, Malta, Portugal, Romania, and Slovenia.
19 Cyprus, France, Greece, Italy, Malta, Portugal, Slovenia, and Spain.
20 BORTEC Study, p. 105.
21 BORTEC Study, pp. 98–99.
22 COM (2007) 575 final.
23 See "Maritime surveillance", European Defence Agency, available at: http://www.eda.europa.eu/otheractivities/maritimesurveillance.

its *'non-refoulement'* obligations.[24] In a separate case at the European Court of Justice (ECJ) brought by the European Parliament, the Advocate General has recently recommended the annulment of the guidelines for FRONTEX joint operations.[25] Although the case is based on a procedural challenge following the European Commission's decision to exclude the European Parliament and EU Council from the legislative process, the ECJ's Advocate-General acknowledged that the procedure had apparently been used precisely because of disagreements among the member states regarding the applicability of the *non-refoulement* principle to extra-territorial operations, and the determination of the point of disembarkation for persons intercepted or rescued.[26] The rules adopted by the Commission as an amendment to the Schengen Borders Code state that on joint operations,

> "priority should be given to disembarkation in the third country from where the ship carrying the persons departed or through the territorial waters or search and rescue region of which that ship transited and if this is not possible, priority should be given to disembarkation in the host Member State unless it is necessary to act otherwise to ensure the safety of these persons".[27]

That Malta has refused to host FRONTEX operations because it believes the guidelines would oblige it to take in persons in distress, while human rights advocates have criticised the rules for encouraging *refoulement* shows how ambiguously the rules have been drafted. A second, linked consideration is the overriding obligations of European ships' captains to go to the aid of irregular migrants in distress at sea under international law and the similarly ambiguous procedures for initiating and conducting search-and-rescue operations.

These debates are important in the context of EUROSUR because of the potential for its new surveillance technologies to be used in pursuit of either aim: preventing the arrival of migrants and refugees, or search-and-rescue operations to address the appalling death toll in the Mediterranean among people in ill-equipped or overloaded boats. While the priority attached to either objective is a core test of the legitimacy of the EUROSUR system, there is clearly a tension between the issues of interception, push-back and search-and-rescue. The reluctance on the part of all EU member states to take responsibility for refugees and asylum applicants is contributing to both a preference for push-back operations and an apparent reluctance to step-up search-and-rescue operations because of corresponding disagreements about what to do with the rescued.

This political intransigence has had deadly consequences. In March 2012 the Council of Europe published a damning report on the death of 63 people left starving, adrift in the Mediterranean after their distress calls went unanswered for days – despite the close proximity of NATO air and sea assets and an alert from the Italian Coastguard.[28] The Council of Europe report found there had been a "collective failure" among NATO and European coastguards and called for further investigations. In April, human rights groups commenced related legal action against the French Ministry of Defence, with further cases expected to follow.

---

24 *Hirsi and others v Italy*, case no. 27765/09.

25 Council Decision 2010/252/EU of 26 April 2010 supplementing the Schengen Borders Code as regards the surveillance of the sea external borders in the context of operational cooperation coordinated by Frontex (Sea Borders Rule).

26 Opinion of Advcoate-General Mengozzi, 17 April 2012, Case C-355/10, *European Parliament v Council of the European Union* at para. 64.

27 Council Decision 2010/252/EU, at Article 2, Part II.

28 "Lives lost in the Mediterranean Sea: who is responsible?", Council of Europe Parliamentary Assembly, 29 March 2012, available at: http://assembly.coe.int/CommitteeDocs/2012/20120329_mig_RPT.EN.pdf.

2.1.1 The EUROSUR roadmap

In February 2008 the European Commission produced a Communication on EUROSUR in which it announced that it was to begin developing the EUROSUR system, rendering somewhat hollow its invitation to the European Parliament to "discuss the recommendations put forward in the Communication."[29] Eight specific steps were envisaged within these three phases (see Box 1). In addition, the Commission announced its intention to produce a Technical Study to design the system architecture and estimate the approximate financial costs. This has resulted in the European and national parliaments being presented with something of a *fait accompli*, insofar as being asked what kind of new border surveillance systems (if any) should be introduced at the European level.

Box 1: The EUROSUR roadmap[30]

PHASE 1: Upgrade and extend national border surveillance systems and interlinking national infrastructures in a communication network

- **Step 1**: Establish National Coordination Centres in the member states with "the capacity to provide situational awareness of conditions and activities along the external borders as well as all the necessary tools to react accordingly."
- **Step 2**: Set up a secure computerised communication network to "exchange data 24 hours a day in real-time between centres in Member States as well as with FRONTEX."
- **Step 3**: Increase EU financial and logistical support for neighbouring third countries for the setting up of border surveillance infrastructure.

PHASE 2: Develop and implement common tools and applications for border surveillance at EU level

- **Step 4**: Conduct research and development to improve the performance of surveillance tools, in particular earth observation satellites and UAVs.
- **Step 5**: Development of shared surveillance tools, with FRONTEX acting as a facilitator.
- **Step 6**: Develop surveillance systems covering the open seas to provide a "Common pre-frontier intelligence picture."

PHASE 3*:* Create a common monitoring and information sharing environment for the EU maritime domain that allows all relevant data from national surveillance, new surveillance tools, European and international reporting systems and intelligence sources to be gathered, analysed, and disseminated in a structured manner between the relevant national authorities.

- **Step 7**: Establish an integrated network of reporting and surveillance systems for border control and internal security purposes covering the Mediterranean Sea, the southern Atlantic Ocean (Canary Islands), and the Black Sea; common pre-frontier intelligence pictures could be developed to combine intelligence information with that obtained from surveillance tools.
- **Step 8**: Create an integrated network of all European maritime reporting and surveillance systems covering all maritime activities, including safety, protection of the marine environment, fisheries control, and law enforcement.

29 COM (2008) 68 final.
30 Idem.

2.1.2 The draft EUROSUR Regulation

The draft EUROSUR Regulation was published by the European Commission in December 2011.[31] It certainly could have been produced much sooner after the Lisbon Treaty had entered into force, allowing for a proper debate to have taken place ahead of the substantial steps taken to implement the EUROSUR roadmap (these are discussed further in section 4).

The purpose of EUROSUR is – as described in the impact assessment and reflected in Article 1 of the proposal – "to improve the situational awareness and reaction capability of Member States and the Agency when preventing irregular migration and cross-border crime at the external land and maritime borders." The preamble of the proposal states that the EUROSUR also has the purpose of "protecting and saving lives of migrants",[32] but this is not explicitly provided for in the legislative provisions beyond a general reference to compliance with fundamental rights and "prioritising" the needs of vulnerable groups, including those in distress at sea.[33] The provisions on surveillance, on the other hand, are detailed, wide-ranging, and defined in the broadest possible terms.[34]

In practical terms, as well as establishing a comprehensive European Border Surveillance System based on a complex "system-of-systems" approach,[35] the Regulation would extend the obligations of Schengen states – conducting border checks and surveillance to detect criminal activity and prevent unauthorised migration – with a much stronger requirement to conduct comprehensive "24/7" surveillance of those land and sea borders that FRONTEX designates as high-risk in terms of unauthorised migration. The draft Regulation would also significantly expand the current role and powers of FRONTEX – from conducting such risk assessments and coordinating joint operations to performing surveillance of the seas beyond EU territory through a "Common pre-frontier intelligence picture" based on the sharing of information and intelligence. The Regulation would also oblige *all* participating states – not just those deemed to have high risk or vulnerable borders – to make a

31 COM (2011) 873 final, 12 Dec. 2011.

32 Recital 1.

33 Article 2(3).

34 According to Article 3: (a) "situational awareness" means the ability to *monitor, detect, identify, track and understand cross-border activities* in order to find reasoned grounds for control measures on the basis of *combining new information with existing knowledge*; (b) "reaction capability" means the ability to *perform actions aimed at countering illegal crossborder movements*, including the means and timelines to react adequately to unusual circumstances; (c) "situational picture" means *a graphical interface to present real-time data, information and intelligence received from different authorities, sensors, platforms and other sources, which is shared across communication and information channels with other authorities in order to achieve situational awareness and support the reaction capability along the external borders and the pre-frontier area*; (d) "cross-border crime" means *any serious or organised crime* committed at the external borders of Member States, such as trafficking in human beings, smuggling of drugs and other illicit activities; (e) "external border section" means *the whole or a part of the external land or sea border of a Member State as defined by national legislation or as determined by the national coordination centre or any other responsible national authority*; (f) "pre-frontier area" means *the geographical area beyond the external border of Member States, which is not covered by a national border surveillance system* [emphasis added].

35 See Box 2 on p. 14 for a detailed overview. The European Defence Agency describes a "system of systems" as a set or arrangement of systems that, for reasons of physical distance or of different primary responsibilities, do not lend themselves to fusion into a single system. "A commonality in procedures, databases used, or overall objectives, advise and allow a certain pooling of resources with synergetic effect, without losing physical and organisational independence. This pooling of resources can be made in a centrally organised way, or by an association of peers." Wise Pen Team, "Maritime surveillance in support of CSDP: The Wise Pen Team Final Report to EDA Steering Board", Apr. 2010, p. 48.

substantial investment in the alignment of their own border control systems with EUROSUR's standards and requirements.

The EUROSUR system will link the member states to FRONTEX via a network of National Coordination Centres.[36] The NCCs will be obliged to maintain a National Situational Picture that covers their coastlines and territorial waters "in order to provide all authorities with responsibilities in border surveillance at national level with effective, accurate and timely information which is relevant for the prevention of irregular migration and cross-border crime."[37] The draft Regulation then sets out in some detail how the National Situational Picture is to be organised into three specific events, operational and analytical "layers", each with three or four "sub-layers". At a later date it is planned to link the landlocked member states into the EUROSUR system. The NCCs will be responsible for coordinating the national responses to any threats to security identified by FRONTEX/EUROSUR, effectively extending the mandate of the existing network of NCCs established by those member states who participate in the European Coastal Patrol Network established in 2006.[38] "Voluntary" guidelines for NCCs drawn up by FRONTEX were adopted in 2009[39] and subsequently incorporated into the Schengen catalogue on External Border Control,[40] obliging Schengen states to adopt a national Border Management Strategy, establish an NCC, and develop the surveillance infrastructure enabling participation in EUROSUR. By the end of 2011, 16 out of the 18 member states located at the southern and eastern Schengen external borders had established their NCCs, with the majority of them having become operational in 2011.[41]

The counterpart for the NCCs is the FRONTEX Situation Centre (FSC), which was established in 2008.[42] Information is exchanged between the FSC and NCCs via a secure computerised communication network. This allows FRONTEX to combine the "national situational pictures" into a multi-layered European Situational Picture, which shall also include "information collected … from *other* relevant European and international organisations [and] *other* sources."[43] FRONTEX shall also be responsible for maintaining the Common Pre-Frontier Intelligence Picture, which basically amounts to the surveillance of non-territorial waters and the territories of third states. The Common Pre-Frontier Intelligence Picture shall be comprised of data provided by NCCs, immigration liaison officers in third countries, *other* relevant European and international organisations, third countries, and *any other sources*. FRONTEX will also be responsible for the "common application of surveillance

36 Under the terms of their opt out of Schengen provisions, the UK, Ireland and Denmark will not be part of EUROSUR. Norway, Iceland, Switzerland and Liechtenstein, which are not EU member states but are part of the Schengen area, will participate.
37 Article 9. The National Situational Picture "shall be composed of" information fed from a myriad of existing surveillance systems: national border surveillance systems; stationary and mobile sensors operated by national authorities (radars etc.); patrols on border surveillance and other monitoring missions; local, regional, and other coordination centres; other relevant national authorities and systems; the Agency; National Coordination Centres in other member states and in third countries; regional networks with neighbouring third countries; ship-reporting systems, such as the AIS and the VMS; and any other sources.
38 Article 5.
39 FRONTEX decision of 10 Mar. 2009, revised 23 Nov. 2010.
40 Council doc. 7864/09.
41 SEC (2011) 1536 final, 12 Dec. 2011, pp. 15–16.
42 See "FRONTEX one stop shop", FRONTEX, available at: https://foss.frontex.europa.eu/.
43 Article 10, draft Regulation [emphasis added].

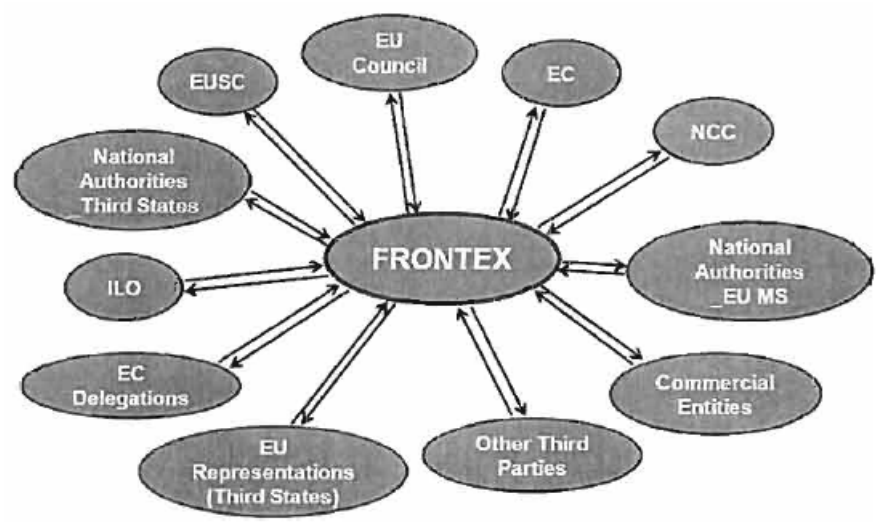
tools" including satellites, ship reporting systems, vessel monitoring systems, and "sensors mounted on *any* platforms, including manned and unmanned aerial vehicles."[44]

Finally, the Explanatory Memorandum states that "cooperation with neighbouring third countries is crucial for the success of EUROSUR." This cooperation will build on earlier efforts to secure the cooperation of countries of origin and departure of migrants and refugees bound for Europe, specifically the countries of North and West Africa, by incorporating them into the information sharing system. EU member states had developed sophisticated cooperation frameworks for the exchange of information, return of 'illegal' migrants and policing of North and West African coastal waters to prevent "unauthorised departure" – a severe distortion of the Universal Declaration of Human Rights' guarantee that *everyone* must have the right to leave *any* country.[45] The cooperation agreements, which included the provision of equipment and expertise from EU member states, were particularly advanced in respect to Gaddafi's Libya,[46] Ben Ali's Tunisia and the Kingdom of Morocco, but since they are based on bilateral treaties (for example between Italy and Libya or Spain and Morocco), they were beyond the scope of democratic or judicial control at the European level. With prior agreements in disarray following the events of the 'Arab Spring', the European External Action Service has recently launched a "needs assessment missions for border management" in Libya.[47] In addition to the bilateral agreements, EU member states have established multilateral, regional migrational control networks such as "SEAHORSE" (see further section 4.3.2); these too are outside of the scope of the formal EU framework.

The EUROSUR legislation simply provides for the participation of third states and regional networks in the EUROSUR communication network but it is largely silent on how information will be used in practice. These operational decisions will be left to FRONTEX's day-to-day control. The draft Regulation also provides for participation in EUROSUR of EUROPOL, the Maritime Analysis and Operations Centre–Narcotics and the Centre de Coordination pour la lutte antidrogue en Méditerranée, the European Maritime Safety Agency, the European Fisheries Control Agency, and other EU agencies and international organisations.[48] We are concerned that a potentially limitless amount of third parties – coupled with the lack of meaningful oversight on the sharing of data between these parties – implies that "function creep" will be built into the EUROSUR system from the outset.

44 Article 12.
45 Article 13.
46 "Dirty deals and unprincipled politics", Transnational Institute, March 2011, available at: http://www.tni.org/interview/dirty-deals-and-unprincipled-politics.
47 EEAS, EU Launces a needs assessment mission for border management in Libya, available at http://eeas.europa.eu/libya/docs/2012_lybia_border_management_en.pdf
48 Article 17.

Figure 2: "Operational nodes" in the Common Pre-Frontier Intelligence Picture[49]

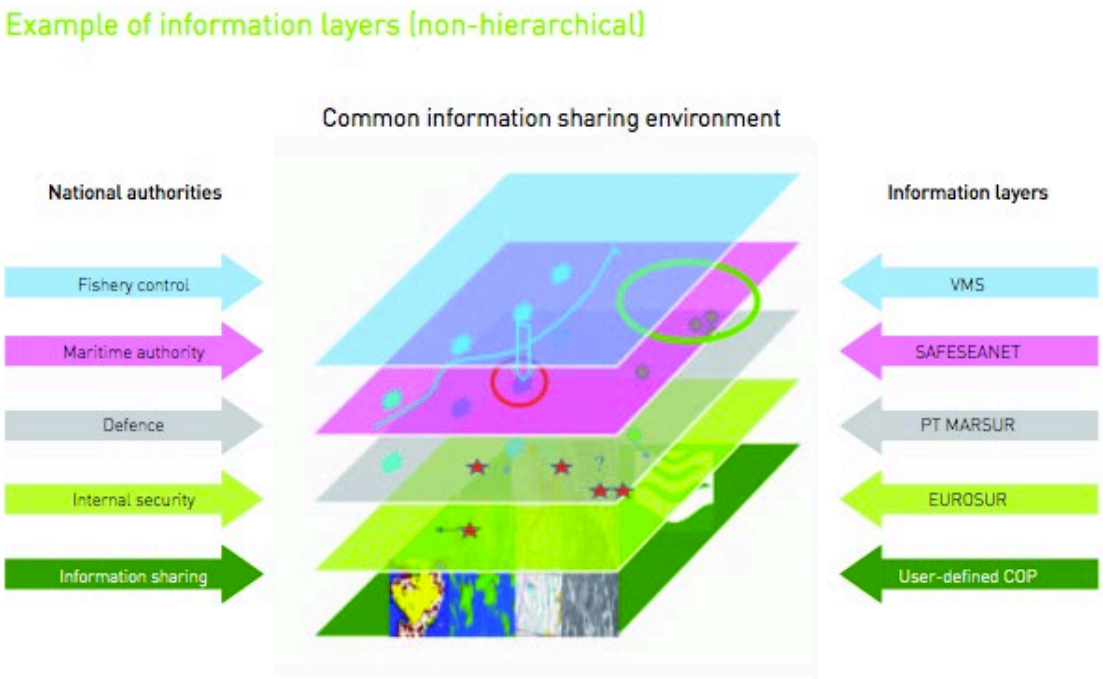


2.1.3 Beyond border control: integrated maritime surveillance

In October 2009 the European Commission produced a follow-up to its earlier Communication on an "integrated maritime policy", with another entitled "Towards the integration of maritime surveillance: A Common Information Sharing Environment [CISE] for the EU maritime domain."[50] This was followed a year later by a "Draft Roadmap towards establishing [CISE] for the surveillance of the EU maritime domain."[51] These two documents propose that EUROSUR is ultimately integrated into a broader system at the disposal of a host of national and international agencies, including those responsible for "Maritime Safety (including Search and Rescue), Maritime Security and prevention of pollution caused by ships; Fisheries control; Marine pollution preparedness and response; Marine environment; Customs; Border control; General law enforcement; Defence."

49 Source: ESG, "EUROSUR Technical Study – Subproject 3 Final Report – Common Pre-frontier Intelligence Picture", Jan. 2010, p. 59.
50 COM (2009) 538 final, 15 Oct. 2009.
51 COM (2010) 584 final.

Figure 3: EUROSUR and the Common Information Sharing Environment[52]



While a full analysis of the potential components of the Common Information Sharing Environment is beyond the scope of this report, Box 2, describes some of the main "information layers" and stakeholders that are likely to be integrated into EUROSUR/CISE.

According to the draft CISE roadmap, the "common needs to most of the [maritime surveillance] User Communities are to obtain an enhanced basic maritime situation awareness picture … This picture may be composed by data stemming from *a combination of systems and sensors detecting cooperative and non-cooperative targets of any size.*"[53] This is essentially the rationale for EUROSUR as set out in FRONTEX's BORTEC study. It is also clear that the European Commission envisages EUROSUR providing this capacity to a wide CISE user community, describing the European Border Surveillance System as "Integrating the needs and tools of all aspects of maritime surveillance in one common information sharing environment along the lines set out in this [CISE] Communication."[54] As to the purpose of the new Common Information Sharing Environment, the draft roadmap states that it will be used:

> (a) To obtain data as regards *illegal activities and threats* impacting on both internal and external EU security, and *involving any type of vessel*. Such information is gathered essentially by coast guards, border guards, police services, and *defence forces*.
>
> (b) To obtain specific catch information, combining it with position information of fishing vessels to *fight against illegal fishing*.

52 COM (2010) 584, p. 5.
53 Emphasis added.
54 SEC (2009) 1341 final, p. 3.

(c) To *obtain advanced electronic data concerning all goods entering and leaving the EU customs territory* in order to enable a pre-assessment of the safety and security of goods.[55]

Insofar as the European Commission clearly envisages the use of EUROSUR for the purposes of fisheries control and for customs enforcement, as well as by national military forces, this extended scope and purpose should have been set out in the draft legislation, not least because of its potential impact on fundamental rights. Instead, as noted above, the proposal simply provides for an open-ended list of datasets and agencies to be integrated into the system. There may or may not be very good reasons for using EUROSUR for the above purposes, but these should be clarified from the outset. It is otherwise difficult to see how the legislation establishing the EUROSUR system can be adopted in the knowledge that the system's scope and purpose could be much wider than those to which the EU legislature is being asked to consent.

Box 2: EUROSUR – A system of systems

International Maritime Organisation requirements: AIS and LRIT

The International Maritime Organisation requires cargo and passenger ships to transmit data that can be read by coastal authorities using radar and satellite. Automatic Identification Systems (AIS) broadcast information from ship-borne transponders, including the identification, position, speed, course, and basic information about the ship and its cargo.[56] Long Range Identification and Tracking (LRIT) requires the periodic transmission of data concerning the identity and position of vessels via satellite. The data is picked up by LRIT Data Centres, although the International Maritime Organisation stipulates that only the flag state, the contracting (port) state of the ship's destination, and coastal states within a distance of 1,000 nautical miles have access to the data.[57] AIS and LRIT data is to be incorporated into the EUROSUR system.

EU fisheries control and Vessel Monitoring and Detection Systems (VMS/VDS)

Vessel Monitoring Systems (VMS) were created as part of the EU Common Fisheries Policy. Legislation requires each member state to establish a satellite-based VMS to monitor the position and movement of fishing vessels.[58] VMS provide reports on the location of a vessel at regular intervals and can be used to provide information on its speed and course. Monitoring authorities use VMS data to police access to fishing zones and verify that vessels hold the necessary licences and quotas to fish in the relevant area. In 2009 the Fisheries Control legislation was amended so that the Vessel Monitoring System became the Vessel Detection System (VDS) and that VMS, VDS, and AIS data collected for fisheries control can be transmitted to Commission agencies and other public authorities of the member states "engaged in surveillance operations for the purpose of maritime safety and security, border control, protection of the marine environment and general law enforcement."[59]

55 COM (2010) 584, p. 4 [emphasis added].
56 AIS became mandatory for all ships of 300 gross tonnage and upwards engaged on international voyages, all cargo ships of 500 gross tonnage and upwards, and all passenger ships irrespective of size on 31 Dec. 2004.
57 LRIT became mandatory for passenger and cargo ships of 300 gross tonnage and upwards on international voyages and mobile offshore drilling units on 31 Dec. 2008.
58 Directive 2002/59/EC. Since 1 January 2005 all Community vessels exceeding 15 metres overall length are subject to VMS, excluding those that are used exclusively for aquaculture and operating exclusively inside the baselines of member states. Third-country vessels subject to VMS are obliged to have an operational satellite tracking device installed on board when they are in Community waters.
59 Articles 11 and 12, Directive 2009/17/EC.

SAFESEANET

SAFESEANET is a vessel traffic monitoring and information system run by the European Maritime Safety Agency (EMSA), which enables the EU member states plus Norway and Iceland to provide and receive information on ships, ship movements, and hazardous cargoes in order to prevent marine pollution, police the transport of hazardous materials, and detect health and safety breaches.[60] SAFESEANET includes a dedicated EU Vessel Traffic Monitoring and Information System that combines AIS position reports and data supplied in accordance with other EU Directives, such as those relating to port reception facilities for ship waste control inspections. According to EMSA, SAFESEANET tracks 12,000 ships in EU waters every day and records 100 million AIS positions every month. SAFESEANET was established as a Central Index System that functions like a telephone switchboard insofar as it stores only references to the data locations and not the actual data itself.

In 2010 EMSA added a dedicated ship-tracking module to the SAFESEANET information system. The SAFESEANET Tracking Information and Exchange System combines information from Port Notification messages, Ship Notification messages (based on AIS data), Hazardous Materials Notification messages, and Incident Reports. According to EMSA Executive Director Willem de Ruiter, "This approach will give Member State users a whole range of important new capabilities to work with … Instead of just accessing a database, they will be able to see the whole near-real-time situation for the EU displayed on a map right in front of them, and to select all ships, ports, sea areas and many other elements at the click of a button. Much better still, we will soon be in a position to offer an integrated display system which will be able to identify and locate ships anywhere in the world and also show the EU pollution and accident pictures. The user base is expanding all the time, with port state control officers being among the latest to join the system."[61]
In 2010 a pilot project on merging data from the EU's VMS and SAFESEANET information system was launched in the Western Mediterranean. The project is led by EMSA with participation from Spain, France, Italy, FRONTEX, and the Community Fisheries Control Agency. The Commission has stated it intends to amend the Directive governing the use of SAFESEANET in 2013 to allow its incorporation into EUROSUR.

e-Maritime

The EU's e-Maritime initiative aims to foster the use of advanced information technologies in the maritime transport sector by funding the development and take-up of the latest enabling ICT technologies for the improvement of maritime transport services. Ports in particular use a variety of automated information systems for the recording of information regarding ships, cargo, crew, and so forth. "The EU e-Maritime envisages promoting interoperability in its broader sense. It aims to stimulate coherent, transparent, efficient and simplified solutions in support of cooperation, interoperability and consistency between Member States and transport operators."[62]

e-Customs

The EU's "electronic customs" project aims to replace paper format customs procedures with EU-wide electronic ones in order to enhance security at the EU's external borders and to facilitate trade. It should therefore benefit both businesses and citizens.[63] Customs Information Systems include the dedicated EU Customs Information Systems, a new Computerised Transit System, an Automated Export System, and an Economic Operators' Registration and Identification System.

Counter drug trafficking and maritime piracy initiatives

60 Directive 2002/59/EC (as amended by Directive 2009/17/EC) on the establishment of a Community vessel traffic monitoring and information system. See also "SafeSeaNet", European Maritime Safety Agency, available at: http://www.emsa.europa.eu/operations/maritime-surveillance/safeseanet/113-safeseanet.html.
61 "EMSA Launches New, Map-based Shipping Surveillance System", EMSA Press Release, 10 March 2010, available at: http://www.emsa.europa.eu/news-a-press-centre/external-news/download/296/2/23.html.
62 See "e-Maritime", European Commission, available at: http://ec.europa.eu/transport/maritime/e-maritime_en.htm.
63 See "Electronic customs", European Commission, available at: http://ec.europa.eu/taxation_customs/customs/policy_issues/electronic_customs_initiative/index_en.htm.

Two operational task forces have been established by the member states to combat drug trafficking by sea. The Maritime Analysis and Operation Centre–Narcotics was established in 2007 by Spain, France, Ireland, Italy, the Netherlands, Portugal, and the United Kingdom to "enhance criminal intelligence and coordinate police action on the high seas, with a view to intercepting vessels carrying cocaine and cannabis," and naval and law-enforcement bodies (police, customs) collaborate with it.[64] The Centre de Coordination pour la Lutte Anti-Drogue en Méditerranée is a law enforcement initiative to curb drug smuggling in the Western Mediterranean and was launched under the French Presidency in 2008 – it is open to all EU member states and North African countries in the region for bilateral intelligence-sharing to combat drug trafficking.[65] Both organisations are mentioned in the draft EUROSUR Regulation.[66] The European Commission has also suggested that EUROSUR's "situational picture" could be used for counter-piracy initiatives. The EU's Critical Maritime Routes programme was launched in 2010 with pilot projects in the Gulf of Aden and Bab El Mandeb Straits as well as the Straits of Malacca and Singapore. It envisages support for surveillance and protection measures for Community vessels sailing through areas prone to piracy.[67]

National and EDPS military operations

The European Defence Agency launched its Maritime Surveillance project in 2006 with the aim of creating "a network using existing naval and maritime information exchange systems" in order "to avoid duplication of effort and the use of available technologies, data and information; to enhance cooperation in a simple, efficient and low-cost solution for civil-military cooperation; and to support safety and security."[68] A Maritime Surveillance project working group on maritime surveillance networking that was established in 2006 is developing "naval maritime interoperability by developing agreed standards and protocols using gateways and existing systems rather than a dedicated new system." In 2009 the European Defence Agency contracted a Wise Pen Team, comprising five retired three-star admirals from five EU naval states to make the case for Maritime Surveillance in Support of the EU Common Security and Defence Policy.[69] As the military takes on more and more policing roles – such as countering drug trafficking, piracy and even counter-terrorism – its demand for access to EU maritime surveillance assets such as EUROSUR is likely to increase.

64 See "Maritime Analysis and Operation Centre–Narcotics", European Monitoring Centre for Drugs and Drug Addiction, available at: http://www.emcdda.europa.eu/about/partners/maoc.
65 SEC (2009) 1341 final, p. 5.
66 Article 17, draft Regulation.
67 See "Building regional maritime capacities", European Union External Action Service, available at: http://eeas.europa.eu/piracy/regional_maritime_capacities_en.htm.
68 "Maritime surveillance", European Defence Agency, available at: http://www.eda.europa.eu/otheractivities/maritimesurveillance.
69 Wise Pen Team, "Maritime surveillance"; see also Wise Pen Team, "Maritime surveillance in support of CSDP: The Wise Pen Team Progress Report", Dec. 2010.

2.2 The EU "smart borders" initiative

In contrast to EUROSUR, there are as yet no legislative proposals on the EU's smart borders initiative. This makes an assessment of this initiative a more challenging exercise, because there is no detailed description of the exact purpose, set-up, functions, or modalities of an Entry-Exit System or Registered Traveller Programme. In this section we will briefly sketch the origin of the initiative, and highlight certain aspects that might be included in the final legislative proposal and that would require closer scrutiny.

The idea of a European Exit-Entry System, loosely modelled on the US-VISIT system, was first floated in December 2004, when the European Policy Evaluation Consortium presented its extended impact assessment of a (then) future Visa Information System (VIS).[70] The EES was described as a computerised system that would allow the monitoring of the movements of all visa holders – from the visa application stage through to their arrival at the external border and ultimate departure from the Schengen area. The identity of all third-country nationals would be checked, but biometric data would only be required from nationals of countries subject to EU visa requirements. This data would be gathered at the consular posts and verified when the visa holder arrived at an EU entry point; it would then be checked as to whether they were the same person who received the visa, and whether there was any information about their involvement in terrorism or crime. Upon leaving the country, the visitor would be required to confirm their departure at the exit points, which would demonstrate their compliance with immigration requirements, facilitate their future travels, but also identify people who overstay their visas ("overstayers"). At this stage there was no link between the EES and the RTP. The 2004 impact assessment noted that the creation of such a system would be very costly, have a significant human rights impact, and go "far beyond the objective of improving the implementation of Common Visa Policy through better exchange of information between Member States and indeed other objectives set by the Council for a VIS."[71]

Having agreed on the creation of a biometric Visa Information System, the idea of an EES remained on the backburner – not least, according to the Commission, because the "internal security and intelligence communities" saw some shortcomings related to VIS: it only dealt with TCNs on the so-called "blacklist" of countries that require an advance visa; there was no similar mechanism to control the identity or the legality of the entry of other categories of TCNs, such as holders of long-stay visas or residence permits, or TCNs that are not subject to a visa requirement (those on the so-called "white list").[72] VIS was also unable to monitor the entry of TCN visa holders or verify whether they had departed before the expiry of their right to stay.[73] Later in 2005 the Commission suggested that an EES could also be used as a register of temporary (seasonal) workers from third countries, which could keep track of those TCNs that had left the EU at the expiration of their temporary

70 European Policy Evaluation Consortium, "Study for the extended impact assessment of Visa Information System", Dec. 2004.
71 Idem, pp. 31–37.
72 The "black list" and "white list" countries are set out in Regulation 539/2011/EC (as amended).
73 COM (2005) 597 final, p. 6. In 2006 the Commission stressed that SIS II would also not be a sufficient tool to replace the need for an EES, since the alerts registered in respect of third-country nationals in SIS II "only concern persons to be refused entry into the Schengen area, which is a very limited number compared to those required to be registered by an entry-exit system", COM (2006) 402 final, p. 6.

residence/work permit and those who had "overstayed."[74] It was also becoming clear, however, that collecting biometric data from all TCNs entering the Schengen area would result in longer waiting lines at the borders. The long-term scenario of an EES was therefore linked to the introduction of a border-crossing facilitation scheme for frequent border crossers. At the end of 2006, the European Council invited the Commission to report before the end of 2007 on "how to improve access control, including on the feasibility of establishing a generalized and automated entry-exit system for this purpose" in order to enhance border control and to allow persons to be identified reliably.[75]

In February 2008 the Commission produced its "smart borders" communication, outlining three potential measures to meet the dual objectives of enhancing security of the EU and facilitating travel for third-country nationals: (1) the creation of a Registered Traveller Programme to facilitate the travels for "bona fide" registered travellers, (2) the introduction of an Entry-Exit System, and (3) the introduction of a European Electronic System of Travel Authorisation.[76] Together with the accompanying impact assessment, these documents are the most detailed public records that explain the use and potential functionalities of the system. The French and Czech presidencies of the EU treated the creation of an EES as a priority and the proposals were received enthusiastically by the EU Council Working Party on Frontiers.[77] In 2009 the Commission stated that it was in the process of conducting another impact assessment for both the EES and the RTP and announced that it would present a legislative proposal "by mid-2011" with a view to the systems becoming operational in 2015.[78] "Proposals for an entry/exit system" alongside a fast-track registered traveller programme were also included in the Stockholm Programme, with a view to the systems becoming operational "as soon as possible".[79]

Despite these commitments, the appetite among the member states to create another large-scale information management system in the area of Justice and Home Affairs seems to have been decreasing, perhaps because the purported "migratory pressure" from the 'Arab Spring' has failed to materialise.. More importantly, the ongoing financial crisis has placed increased pressure on national and EU budgets. The failure to implement the Schengen Information System II (see Box 3), which has proved much more expensive than initially envisaged, has compounded this problem. Some – but certainly not all – member states have also been concerned from the outset that systems of the magnitude of EES and RTP require strict data protection standards, and they understand that this is a

74 COM (2005) 669 final, pp. 10–11.
75 Council doc. 16879/06, p. 9. During the Portuguese Presidency in 2007, the use of new technologies for enhancing the EU's border management was further discussed at the Informal Strategic Committee on Immigration, Frontiers and Asylum on 4–5 Sep. 2007 and the Informal Justice and Home Affairs Council on 1–2 Oct. 2007.
76 COM (2008) 69 final, pp. 4–5. Initially it was suggested that a European ESTA would only apply to TCNs who are not subject to the visa requirement. They would be requested to make an electronic application, thereby supplying, in advance of travelling, data identifying the traveller and specifying the passport and travel details.
77 The Working Party on Frontiers discussed the proposals during 2008 and 2009. Finland, Hungary, the United Kingdom, the Netherlands, Germany, and Slovakia presented their national EES or RTP in the Working Group, and two questionnaires were circulated among the members of the Working Group, first to assess their opinions on the need an functions for an EES for TCNs in the Schengen area, and secondly to gather some relevant statistical information. Between 31 Aug. and 6 Sep. 2009 a "data collection exercise" was held in order to gather comparable data on entries and exits of different categories of travellers at different types of external borders in order to help the Commission to submit a legislative proposal by early 2010.
78 SEC (2010) 1480 final, p. 13.
79 Council doc. 16484/09, p. 55.

sensitive issue for the European Parliament. All of this was acknowledged at an informal meeting of the EU Justice and Home Affairs Council in July 2011 in Sopot, Poland, where ministers stated that "before embarking on new projects of this kind, the Commission and the Member States must first ensure there is a shared understanding and a strong commitment and ownership towards working together to deliver on commonly agreed objectives. Therefore Ministers are invited to express their views on the justification for the system, notably the added value in light of the technological implications (including in relation to data protection) and the cost."[80] The Commission was then invited to present another Communication that would "reflect" these discussions.

In its October 2011 Communication on smart borders, the European Commission set out several options for further consideration, while stating that it did not intend to "prejudge any future specific proposals", which would be accompanied by a full impact assessment in due course. Two things were clear, however. Firstly, the new EU Agency for Large-scale IT Systems would be responsible for the development and operational management of the systems in order "to limit possible risks such as those which have arisen during the development of the SIS II and the VIS."[81] Secondly, the European Electronic System of Travel Authorisation for visa-exempted third-country nationals was no longer under consideration (and is not discussed further in this paper), since its potential contribution to enhancing the security of the member states "would neither justify the collection of personal data at such a scale nor the financial cost and the impact on international relations."[82] Finally, in February 2012, the Danish Presidency hosted a conference on "Innovation Border Management", which was intended to provide input to the Commission, which was now expecting to deliver its legislative proposal on smart borders in June 2012. At the time of writing, it seems unlikely that the proposal will be presented before the summer.

2.2.1 Entry-exit system

The general purpose of the EES would be to identify overstayers, that is, persons who enter the EU legally with a valid travel document and/or visa, but who become illegal migrants when their legal entitlement to stay expires. This category of overstayers is said to constitute "the biggest category of illegal immigrants in the EU".[83] In its "border package" of 2008, the Commission had suggested that the EES would automatically register the time and place of entry and exit of third-country nationals who are admitted for a short stay (up to three months) in order to verify their exit and identify them if they overstayed.[84] In this case, an alert would automatically be sent to relevant national

80 Conclusions of the Informal Meeting of the Justice and Home Affairs Ministers in Sopot, 18–19 July 2011, p. 2.
81 COM (2011) 680 final, p. 13.
82 Idem, p. 7. This might change in the future however. Recently the German Minister of Interior expressed interest again in a European ESTA, rather than creating an EES. Frankfurter Rundschau, EU-Innenminister beraten über Salafisten, 18 May 2012, available at http://www.fr-online.de/politik/g-6-treffen-in-muenchen-eu-innenminister-beraten-ueber-salafisten,1472596,16066774.html
83 COM (2008) 69 final, p. 5. According to the Commission, reliable data on the number of irregular immigrants within the EU is not available, but conservative estimates from 2008 vary between 1.9 and 3.8 million. COM (2011) 680 final, p. 4.
84 Currently the stamping of the travel document is the sole instrument indicating the dates of entry and exit at the disposal of border guards and immigration authorities. These stamps are said to be "often difficult to interpret" and "may be illegible or the target of counterfeiting". SEC (2008) 153 final, p. 10.

authorities if a person's stay expires and no exit data is captured by the EES.[85] This would allow national authorities to take unspecified "appropriate measures", which could include fines or issuing an expulsion order. The Commission argued that the EES would deter TCNs from overstaying and also provide information "for operational purposes" on patterns of overstaying (e.g., travel route, fraudulent sponsors, country of origin, and reasons for travelling) as well as data on migration flows and overstayers for visa policy purposes.[86]

At this point in time, it is not clear yet which data would be collected by a potential EES. To reach its goals of identifying overstayers, the system would at least need to record and store the following information in order to track and calculate the time spent in a given area and identify the overstayer: (a) border-crossing point of entry and exit; (b) date and time of event; (c) type of travel document(s), including number of document and issuing country; (d) the traveller's personal details extracted directly from the travel credential, including name, sex, and date of birth.

In its last Communication on smart borders, in 2011, the Commission suggested that the "best way forward" would be to establish the EES in stages and begin by recording only alphanumeric data (e.g., name, nationality, and passport number) and introducing biometric identifiers (fingerprints and a digital image of the face) at a later date.[87] However, a majority of member states "expressing a position" on the issue at a Council Meeting in December 2011 had wished to introduce biometrics into the EES from the outset.[88] It is unclear how long the data would be retained. Discussions seem to suggest a period between six months and the VIS standard of five years. Data of a TCN who has entered and left the territory in accordance with the rules are likely to be retained for this period in order to establish and map "travel patterns." It remains to be seen how the retention of this type of data for a prolonged period of time will be in accordance with the purpose limitation principle, a fundamental principle of EU data protection law. In 2008 the Commission further envisaged "an automated housekeeping procedure which cleans up aged records according to the retention times".[89]

The Commission has stated explicitly that "the data generated by the entry/exit system would be used by the competent immigration authorities."[90] In the accompanying impact assessment the Commission envisages the possibility of other authorities having access to the overstayers database: "various authorities may, according to an agreed legal framework and when necessary, access and use the information on the different target groups that is available in the database." The Commission stipulates that this should only apply "in exceptional circumstances where duly authorised law enforcement authorities seek with good cause, evidence on the travel histories of

85 COM (2008) 69 final, p. 7. In 2011 the Commission stressed that the electronic recording of the entry and exit information ideally would have to take place *at central level* instead of at the national level. "Recording the entry and exit information at national level first would necessitate the replication of this information in 27+ other national systems in order to keep them all updated with matching entry and exit records. This might be burdensome and time-consuming when persons enter and leave Schengen via different Member States", COM (2011) 680 final, p. 8.
86 COM (2008) 69 final, p. 8.
87 COM (2011) 680 final, p. 9.
88 Council Doc. 17706/11, p. 2.
89 SEC (2008) 153 final, p. 25.
90 Idem, p. 57, further specifies that this includes "immigration and border control" authorities.

named individuals."[91] However, several Member States seem to be in favour of giving broader access to law enforcement authorities.[92] Eleven member states are currently implementing national entry/exit systems and at least seven of them – Bulgaria, Cyprus, Estonia, Latvia, Hungary, Slovakia, and Poland – seem to provide law enforcement authorities with routine access; they see any EU system as serving the same purpose.[93] Were the EES to be given an explicit internal security function, those same states are also likely to demand the inclusion of data similar to that held in the Visa Information System,[94] such as the address of the accommodation provider or place of residence, the final destination, and the purpose of the trip or stay.[95]

2.2.2 EES relationship to existing EU systems: VIS and SIS II

The explicit objective and purpose of the EES has significant implications for the architecture of the system and its relationship with other EU law enforcement and migration control databases, particularly the Visa Information System and the Schengen Information System (SIS), which the member states and the Commission have been working on upgrading (into SIS II) for more than a decade (see Box 3).

Since an EES will cover the entry and exit data of all third-country nationals, it is logical that data related to TCNs who are subject to a visa requirement will be interoperable with the VIS system.[96] Indeed, the Commission has suggested that a fully operational and developed VIS is "a prerequisite for the implementation of a Smart Borders system."[97] If the sole purpose of an EES is to detect overstayers, the most likely scenario would be that a dedicated EES database that is interoperable with VIS and SIS (II) and has its own central architecture will be developed. The biometric features of the EES will be integrated into the VIS-SIS II architecture via the European Union Biometric Matching System, since the Commission envisages that the Biometric Matching System will be the "central biometric identity assurance tool" for all of its pan-European applications enabling the biometric data held in the VIS database to be checked against fingerprints at points of entry (and potentially exit).[98]

In addition to fingerprint verification in applications like VIS, the Biometric Matching System will also offer fingerprint identification, allowing the searching of large datasets. In this case, only the entry

---

91 Idem, p. 27

92 At the EU conference on innovation border management organised by the Danish Presidency in February 2012 Estonia stated for instance that the EES "should be used by all law enforcement authorities ofr fighting the smuggling, illegal immigration and cross border crime." Malta proposed the "integration of the EES with other national law enforcement systems", with "immediate access" since this would "facilitate investigations related to criminal offences". See also the call of one delegation at a recent meeting of the Law Enforcement Working Party to underline "the need for the current and incoming Presidencies to work on ensuring access for law enforcement" to the EES. Council Doc 10825/12, 5 June 2012, at 2.

93 According to the Commission, 11 member states are currently implementing a national EES (Finland, Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania, Bulgaria, Cyprus, Portugal) COM(2011) 690 final, p. 6.

94 Article 9, VIS Regulation.

95 Council Doc 13267/1/09 REV 1.

96 The member states also appear to favour this option. Council Doc. 17706/11, p. 2.

97 COM (2011) 680 final, p. 7.

98 In 2009 the Commission mentioned the EES in its information management overivew, stating that "based on biometric data verification", an EES would deploy the same biometric matching system and operational equipment as that used by SIS II and VIS. See "European Union – Biometric Matching System" factsheet, available at: http://www.nws-sa.com/biometrics/EU_Matching_CS.pdf.

and exit dates and places would have to be collected for third-country nationals under a visa obligation, without the need to reproduce the information stored in the VIS. The personal data of TCNs who are not under a visa obligation would be stored in this separate database, together with their entry-exit information.[99] An explicit link with VIS could also work in another way. If a person has been flagged as an overstayer in the EES, one of the results could be that a person will not be able to get a visa the next time s/he wants to enter the Schengen area – implying that not being flagged as an overstayer would become a pre-condition for visa approvals.

Box 3: The Visa Information System and the Schengen Information System/SIS II

VISA Information System

The VIS has been operational since 11 October 2011. The central VIS database keeps data from visa applications (including those that are refused) for a period of five years. This includes 10 fingerprints and a digital photograph from persons applying for a visa for the first time, for instance at a consulate of a Schengen state. The first consular posts to be connected to the system were those in Algeria, Egypt, Libya, Mauritania, Morocco, and Tunisia, followed by Israel, Jordan, Lebanon, and Syria. At the Schengen area's external borders, the visa holder's fingerprints are checked in order to verify the identity of the visa holder. After a transitional period, the new EU Agency for Large-scale IT Systems (which will formally become operational in the autumn of 2012) will take over the operational management of VIS. Eventually, the central database is expected to include as many as 80 million visa applications. In addition to the Schengen states' authorities responsible for visa applications, asylum authorities – and in specific cases EUROPOL and national law enforcement agencies – may request access to VIS data for the purposes of preventing, detecting, and investigating terrorist and criminal offences. The Commission acknowledged that it would be sensible to await the "complete and successful rollout" of the VIS to all consular posts and border-crossing points before the EES is implemented in practice.

Schengen Information System

The SIS has been operational since 1995 and has now been implemented in all EU member states except Bulgaria and Romania, as well as Norway, Iceland, and Switzerland. Under the 1990 Schengen Convention, participating states issue "alerts": on people wanted for arrest (art. 95) or in connection with police investigations (art. 99) or criminal proceedings (art. 98); on "aliens" to be refused entry to the entire Schengen area (art. 96); and on lost or stolen vehicles, firearms, identity documents, and bank notes (art. 100). Alerts on persons are held in the SIS for a maximum of 10 years, though they must be reviewed by the issuing state every three years.[100] Border guards and immigration officials then check entrants to the Schengen area against the alerts in the SIS (this is the system against which travel documents are checked upon entry into the Schengen area). Police officers across the Schengen area also have access to the SIS in order to check whether the people they suspect are wanted by other member states (it is up to the member states to decide which national agency can have (partial) access to SIS alerts). Data entered into the SIS includes names and aliases, physical characteristics, place and date of birth, nationality, and whether an individual is armed and violent. An alert specifies which action should be taken against the person; the vast majority of wanted persons consist of third-country nationals who should be denied entry to the Schengen area. Searches in SIS produce a "hit" when the details of a person or object sought match those of an existing alert. There were more than 91,000 hits in 2010, out of a total 35.69 million records. Between 1997 and 2010, a total of 253,640 TCNs were denied entry to EU territory because of SIS data.

99 Purpose limitation restrictions would not allow the VIS to store data on visa-exempt TCNs.

100 This is with the exception of the Article 99 surveillance alerts, which must be reviewed annually. Data relating to identity documents issued and to registered bank notes for a maximum of five years and those relating to motor vehicles, trailers, and caravans for a maximum of three years (Articles 112–113, Schengen Convention).

SIS II

Development and implementation of the "second generation" Schengen Information System (SIS II) has been beset with problems. It is supposed to enhance the capacity and functions of SIS by including more data categories and biometric data such as fingerprints. SIS II will share the Biometric Matching System used by VIS. The first formal tests of the central SIS II system began in May 2011, but it is still unclear when the EU member states will be connected to the new system. In January 2012, the Commission reported that the total budgetary commitments made by the Commission for the central SIS II architecture amounted to more than €135 million.[101] There is also substantial concern about the spiralling costs of upgrading national SIS systems.[102]

The relationship between SIS/SIS II and the proposed EES should also be clarified. If the EES automatically issues an alert to member state authorities on persons whose permission to stay has expired and whose exit has not been confirmed, the Schengen Information System – which effectively allows routine computer checks by police in Schengen states to query international alerts issued by other participating states – is the logical system through which to do this. Without an automated link between EES and SIS/SIS II, the only point at which overstayers (especially those who move to another member state) could conceivably be detected, is when they attempt to leave the Schengen area, which strongly undermines the policing rationale for the EES system. However, issuing automatic alerts on overstayers via the SIS/SIS II and enabling routine police checks to identify them would be unlawful unless substantial changes to the legal framework governing that system were to be made. Article 24 of Regulation No 1987/2006 on SIS II states clearly that "files issued for the purposes of refusing entry or stay must be entered on the basis of a national alert resulting *from a decision taken by the competent administrative authorities or courts*, based on a threat to public policy or public security or to national security." Therefore, unless the SIS Regulation is amended, overstays could not be entered into the SIS (only the resulting expulsion orders when accompanied by a deportation order).[103] As the 'Meijers Committee' of Experts on International Immigration, Refugee and Criminal law has further pointed out, the SIS II regulation currently "leaves room for doubt" as to the legal character of entering an entry ban alert into the SIS, and modifications are needed to clarify the relationship between the current SIS II Regulation and the "entry ban" in the Returns Directive (2008/115/EC).[104]

2.2.3 Registered Traveller Programme

The voluntary EU RTP would seek to reduce the time spent at the border-crossing points for "bona fide travellers". Members of such a programme would benefit from a "simplified and automated" border check after having gone through an extensive pre-screening process. The Commission estimates that an RTP would "speed up the border crossings of 4-5 million travellers per year and lay

101 COM(2011) 907 final, p.8

102 See for instance European Parliament, Report on the proposal for a Council regulation amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System, A7- 0127/2010, 29.04.2010.

103 Directive 2008/115/EC of the European Parliament and of the Council of 16 Dec. 2008 on common standards and procedures in member states for returning illegally staying TCNs [emphasis added].

104 Meijers Committee, Note on the coordination of the relationship between the Entry Ban and the SIS- alert: an urgent need for legislative measures, 8 February 2012, available at 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

the basis for enhanced investments in automated border control technologies at major border crossing points."[105] For those registered passengers, the average time for border-crossings could be cut "from the current 1-2 minutes to below 30 seconds."[106]

Any voluntary Registered Travellers Programme must provide pre-authorised travellers with fast entry to be of any use to those who are interested in applying to the programme; automated gates are seen as the only way of achieving this. At these gates, a document reader would electronically read the biometrics included in the travel documents, or stored in a system or database, and compare them against the biometrics (fingerprints and facial image) of the passengers. The Commission has argued that an RTP system would result in a more "efficient use" of border guards since the automated gates would need little to no supervision by border guards. In its Communication of 2008, the Commission suggested that one border guard should be able to oversee up to 10 automatic border gates in operation.[107] An RTP programme would therefore allow, at least in theory, for the redeployment of existing border guards, enabling them to focus their attention on more "risky" passengers who are not members of the RTP programme. This would create a de facto division between high-risk and low-risk passengers. While any third-country national would be able to apply for this programme at any consulate of any member state, the relaxation of border controls would only apply to low-risk or bona fide travellers who are not deemed to pose a threat to the security of the member states.

In 2008 the Commission listed some factors that could be used to determine which travellers could be determined as "low risk". A traveller was seen as bona fide when s/he travels frequently to the Schengen area for legitimate reasons (for instance travelling on business), has a reliable travel history (the person respects the conditions for their length of stay on each occasion),[108] has proof of sufficient means of subsistence, and holds a biometric passport.[109] The passengers are checked against a number of watch lists to make sure that they are not considered to be a threat to public policy, internal security, public health, or international relations of any of the member states.[110] According to the Commission "other criteria may be imposed."[111] In its 2011 Communication the Commission provided far less information about the pre-screening process, simply stating that this will need to be "sufficiently thorough to compensate for alleviating the border check process."[112] At its informal Council in July 2011, the Council hinted that the vetting criteria could be aligned with the criteria for multiple-entry visa holders.[113]

105 COM (2011) 680 final, p. 12.
106 Idem.
107 At the same time, the Commission notes that it is "extremely difficult" to estimate the impact of the EES and the RTP in practice on the number of border guards and on the travellers' waiting time "as these depend almost entirely on the individual border crossing point and the fact if the Registered Traveller Programme or Automated Border Control system is used at that specific border crossing point or not", SEC (2008) 153 final, p. 34.
108 Note that this condtion would assume that there is a functioning EES system in place (cf. infra).
109 COM (2008) 69 final, p. 6.
110 The Commission foresees that also EU citizens could benefit from such automated gates when crossing the external borders, "except that only random checks of the SIS and national databases can be carried out in accordance with the Schengen Borders Code", COM (2008) 69 final, p. 7.
111 SEC (2008) 153 final, p. 62.
112 COM (2011) 680 final, p. 11.
113 Conclusions of Informal Meeting of the Justice and Home Affairs Ministers in Sopot, 18–19 July 2011, p. 3.

The Commission and the member states prefer to have a central EU RTP database for TCN nationals, rather than having 27 decentralised interoperable systems.[114] In its 2011 Communication, the Commission outlined three options for storing the necessary data of registered travellers, which would allow for an automated verification of the identity of the traveller: (1) storing the alphanumeric and biometric data in a central database, (2) storing the data on a token issued to the traveller, (3) a combination of a central data base with a token containing only a unique identifier (i.e. application number) to be issued to the Registered Traveller.[115] The third option is arguably the best – from a data protection/security perspective – but it is more expensive to develop than the option of a centralised register alone (costs are discussed further in section 4). A majority of the member states have indicated their preference for the centralised storage of data, though some do prefer a combination of a central database with a token.[116]

Currently there are only four operational RTP programmes in major airport and transfer hubs in the EU; three of them (ABG in Germany, Iris in the United Kingdom, and Privium in the Netherlands) use iris scans, while Parafes in France uses fingerprints. There are three further automatic border gate systems in operation that work independently of any RTP system. These are RAPID in Portugal and the Automated Border Control system in the United Kingdom and Spain. All three work on the basis of facial recognition. Most of these systems use only one biometric marker, whereas a future EU RTP is likely to include both facial and fingerprint recognition. Membership of RTPs in the national programmes is generally limited to EU/EEA citizens, and they are not interoperable. Given their high cost and limited value for countries with relatively small numbers of travellers, many member states harbour reservations about the need for an EU-wide Registered Traveller Programme.[117]

114 COM (2011) 680 final, p. 8.
115 Idem, pp. 8–9.
116 Council doc. 17706/11, p. 2.
117 See also reactions of many participants at the EU-conference on innovation border management in Denmark in February 2012.

3 The fundamental rights impact of the EUROSUR and EU "smart border" initiatives

In analysing the impact of the smart borders initiative and EUROSUR proposal on fundamental rights, it is again important to stress that while there is already a legislative proposal for EUROSUR, including a detailed impact assessment, the Commission is still contemplating the exact set-up and modalities of the smart borders package. This section is therefore limited to highlighting notable features of both initiatives that give rise to fundamental human rights concerns.

EUROSUR is based on Article 77(2)(d) of the Treaty on the Functioning of the European Union on the gradual establishment of an integrated management system for external borders. Whereas the development of EUROSUR is well underway, the Commission has emphasised that no work will be done on the development of the EES and the RTP "until the European Parliament and the Council have adopted the legal basis for the systems setting out clearly their specifications."[118] The smart borders initiative will also be based on Article 77 of the Treaty, but it is more likely to be based on Article 77(2)(b), which allows for the adoption of measures concerning the checks to which persons crossing external borders are subject. Any draft legislation must be agreed jointly by the European Parliament and the Council under the ordinary legislative procedure.

The European Commission is required to ensure that all its proposals comply with the Charter of Fundamental Rights.[119] The member states must also implement regulations in accordance with the Charter.[120] From a fundamental rights perspective, there are significant data protection concerns attached to both proposals. The smart borders initiative is likely to entail the creation of at least one centralised EU database containing biometric data, to which a currently unknown number of actors could have access. The EUROSUR proposal, on the other hand, claims that data protection concerns are minimal because the system will not gather large amounts of personal or biometric data or include a central database. Nevertheless, the inclusion of at least some personal information in EUROSUR and the broader Common Information Sharing Environment as well as the potential sharing of personal data with third states and agencies might result in the future in violations of the protection of personal data. Both initiatives can also have an indirect impact on the right to asylum. Last but not least, the EUROSUR proposal further has an explicit human rights aim, insofar as it aims to reduce the loss of lives at sea – though as noted above this needs to be strengthened.

118 COM (2011) 680 final, p. 13.
119 See COM (2005) 172 final, p. 3.
120 See also Preamble 6 of the proposed EUROSUR Regulation.

3.1 The right to privacy and the protection of personal data

Interference by a public authority with individuals' non-derogable rights may be necessary in the interest of national security, public safety, and the prevention of crime. The jurisprudence of the European Court of Human Rights establishes three conditions under which such restrictions may be justified: if it is lawful, if it pursues a legitimate aim, and if it is necessary in a democratic society.[121] The smart borders initiative and the creation of EUROSUR interfere with the right to privacy and the protection of personal data to different degrees. The collection and processing of personal data, including biometrics, is a central feature of the smart borders initiative, while it is considered as only a marginal issue in the set-up of EUROSUR. However, EUROSUR also raises particular privacy and data protection concerns – especially regarding the foreseen use of drones and other means of aerial surveillance, which are currently not properly addressed in the current legislative proposal.

3.1.1 EUROSUR

The Commission stresses that EUROSUR is not intended as a system to regulate the collection, storage, or cross-border exchange of personal data.[122] Instead, EUROSUR focusses on the surveillance of specific geographical areas (borders) and specific activities (illegal border crossings). According to the Commission, "the situational pictures will as a general rule not involve personal data but rather the exchange of information on incidents and depersonalised objects, such as the detection and tracking of vessels."[123] Article 8 of the proposed Regulation also suggests that the situational pictures from both FRONTEX and the National Coordination Centres primarily concern incidents, cross-border crime, crisis situations, the position of national (border security) assets, and strategic and environmental information.

However, currently nine National Coordination Centres – in Bulgaria, Cyprus, Germany, Denmark, Estonia, Spain, Romania, Slovenia, and Slovakia – are allowed to process personal data, and this information can be included in their national situational picture.[124] The description of the different "layers" of the national situation picture further suggests that personal data could be included in a range of scenarios. The required reporting on incidents concerning the illegal border crossings of migrants, trafficking in human beings, or smuggling of drugs in the "events layer"[125] could for instance include personal data on both criminals and victims. When a suspicious vessel is being tracked, data about the ownership of the vessel, its operators, passengers, crew, agents, etc., is highly likely to be processed. The draft Regulation also states quite ambiguously that the events layer can contain information on *"unidentified* and suspect (…) persons present at or nearby the external borders of the Member State concerned."[126] The operational layer of the national

121 The interpretation of Directive 95/46/EC and Regulation (EC) No 45/2001 must depend partly on relevant case law from the European Court of Human Rights; see for instance European Court of Justice, Österreichischer Rundfunk and Others (Joined Cases C- 465/00, C-138/01 and C-139/01, Judgment of 20 May 2003, Full Court, (2003) ECR I-4989).
122 COM (2011) 873 final, p. 3.
123 Article 2, draft Regulation.
124 SEC (2011) 1538 final, pp. 31–32.
125 Article 9.3.a, draft Regulation.
126 Article 9.3.d [emphasis added].

situational picture might also involve information on the border authorities involved in an operation.[127] The analysis layer of the national situational picture can consist of an intelligence picture sub-layer, which can contain undefined "migrant profiles"[128] and an "imagery and geo-data sub-layer, which shall contain reference imagery, background maps, intelligence validation assessments, change analysis (earth observation imagery) as well as change detection, geo-referenced data and border permeability maps."[129] It is as yet unclear whether such images could include images of identifiable persons, but this seems almost certain.

The NCCs can send this information to FRONTEX to create the European Situational Picture,[130] but it is unclear whether FRONTEX can use such personal data in its European Situational Picture. The FRONTEX Regulation specifies that FRONTEX can "use" personal data in the context of joint operations, pilot projects, and rapid interventions for the preparation of risk analyses, but in the results of the risk-analyses, "data shall be depersonalized".[131] It could be argued that the European Situational Picture is similar to such a risk-analysis, especially the "analytical sub-layer", which presents risk-rating trends. The explanatory memorandum of the EUROSUR proposal specifies that in "exceptional cases", personal data may be shared by the member states with FRONTEX, and if such data can be found in a national situational picture, it "may be exchanged between neighbouring Member States only."[132] There is no similar language for the situation when FRONTEX includes personal data in its European Situational Picture, for instance in the "events" and "operational" layers. The extent to which EUROSUR will actually process personal data – and Article 10 of the draft proposal in particular – needs urgent clarification.

Finally, FRONTEX can use information from satellite imagery and drones[133] within the "common applications of surveillance tools" in order to supply the national coordination centres and itself with surveillance information on the external borders and on the pre-frontier area.[134] The definition of an "external border section" suggests that this "section" will be the external land or sea border of a member state as defined by national legislation.[135] The "pre-frontier area" is broadly defined as the geographical area beyond the external border of member states, which is not covered by a national border surveillance system. The impact assessment offers only a negative explanation: The territory of EU member states and associated countries is outside the scope of EUROSUR.[136] This capability raises a whole range of potential privacy and data protection concerns that are currently not addressed in the Regulation.

Besides monitoring the external land borders and the pre-frontier area, two more operational scenarios in which drones could be used have been identified in the context of the European

127 Article 9.5.b.
128 Article 9.6.c.
129 Article 9.6.d.
130 Article 10.2.d indicates that FRONTEX can receive further information from "other sources"; this info might include personal data as well.
131 Article 11c.3.b.
132 COM (2011) 873 final, p. 2.
133 Article 12.3.
134 Article 12.1.
135 The Schengen Border Code states that **"**external borders**"** means the member states' land borders, including river and lake borders, sea borders, and their airports, river ports, sea ports, and lake ports, provided that they are not internal borders.
136 SEC (2011) 1538 final, p. 24.

initiative for Global Monitoring for Environment and Security (GMES): the tracking of vessels on the high seas and the monitoring of selected neighbouring third-country ports and coasts.[137] The monitoring of a port could be done in order to determine if/when a specific vessel has departed. Coasts "with a distance of more than 40 nautical miles from the coasts of EU Member States (beyond the reach of coastal radar stations)" could be monitored by drones in order to recognise "preparatory activities" that might indicate illegal immigration "such as the erection of tents, huts, the gathering of vehicles or boats placed on the beach."[138] GMES also contemplates the use of UAVs "for the detection, classification and identification of at least 80% of all vessels within a pre-designated area (for instance in times of crisis)." The explanatory memorandum to the EUROSUR proposal states the common application of surveillance tools "could be implemented with the support of relevant European space programmes, including the operational Global Monitoring for Environment and Security" (see section 4).[139]

Currently it is not known whether drones used within the EUROSUR framework will have the capability to recognise persons or processes and store personal data. While FRONTEX has demonstrated a great amount of interest in the use of drones, it remains to be seen whether the agency will purchase its own UAVs. According to the 2012 FRONTEX Work Programme, the agency's Research and Development Unit is currently engaged in a nine-month study to "identify more cost-efficient and operational effective solutions for aerial border surveillance in particular Unmanned Aircraft Systems (UAS) with Optional Piloted Vehicles (OPV) that could be used in FRONTEX Joint Operations (sea and land)."[140] It states further that the "Common Surveillance Tools Project" will develop and test a FRONTEX capability for a combined use of satellite imagery and ship-reporting systems for border surveillance in order to provide surveillance-based information to the EUROSUR network. Again "this is to be done using GMES measures (…) and by working in close conjunction to EUSC and EMSA."[141].

The lack of clarity regarding the processing of personal data is also inappropriate given EUROSUR will perform the "border control" function of the EU's wider Common Information Sharing Environment.[142] As noted in section 2.1.3, the CISE will be based on a decentralised information exchange framework interlinking relevant user communities. This is, in turn, based on a principle of "sharing on a need-to-know and responsibility-to-share basis."[143] While most of the data that will be shared is likely to consist of information about the identity and course of boats and ships, it is also possible that personal information related to crews and passengers will be shared.

The Commission has acknowledged the need for a clear legal framework for the exchange of information, "defining at least the nature of the data involved, the capability and the right of the

137 SEC (2011) 145 final, p. 8. The European initiative for GMES is coordinated and managed by the European Commission. This GMES document is preceded by a disclaimer that states that the document does not represent the views of either FRONTEX or the European Commission and "by no means should (…) be interpreted as the draft or final specifications for future operational services."
138 GMES CONOPS doc. version 1.4, 7 July 2011, p. 11.
139 COM (2011) 873 final, p. 2. The Commission mentions GMES as a "relevant programme" for the service for the common application of surveillance tools. COM(2011) 873 final, p. 35.
140 Council doc. 6514/12, p. 97.
141 Idem, p. 99.
142 COM(2010) 584 final, p. 6.
143 EU Council Conclusions, 23 May 2011, p. 2.

data providers and recipients to exchange the data, the purposes (and the methods) of the exchange as well as incorporating the necessary safeguards with regard to the confidentiality and security of (certain) data and the protection of personal data, where this may be relevant."[144] However, according to the CISE roadmap, this will not be addressed until all the other steps towards establishing CISE have been taken, at which point "obstacles to the exchange of the data present in EU legislation must be identified and solutions to overcome them should be explored."[145] This is regrettable, since CISE raises substantial data protection concerns because of the sheer potential scope of its "user community", which includes customs, border control, law enforcement agencies, and defence forces. Data protection concerns should therefore be addressed from the outset and integrated into the design of the system.[146] The Commission stresses that "these layers are managed by the respective owners of the related information at Member States and EU level based on the applicable legal instruments. The competences of national authorities, as well as the mandates of EU Agencies set out in these legal instruments will thus be fully respected."[147] This implies that EUROSUR information could be used, for example, by international law enforcement missions carried out with military assets (for instance, anti-piracy operations). Moreover, where naval forces have assets dedicated to maritime surveillance and/or law enforcement missions, EUROSUR could receive information from defence bodies as well.[148] It is unfortunate to say the least that the EUROSUR proposal does not include a single reference to the CISE system.

3.1.1.1 The need for safeguards

The Commission's EUROSUR proposal only refers to the data protection framework in relation to the exchange of personal data using the EUROSUR communication network in the preamble, and even then does not explicitly mention the collection of personal data, which is likely to take place on some levels within EUROSUR.[149] The (amended) FRONTEX Regulation is the *lex specialis* that applies to FRONTEX activities in this context. Where the FRONTEX Regulation does not provide a "full data protection regime", other data protection provisions of Directive 95/46/EC and Regulation (EC) No 45/2001 apply and – in the framework of police and judicial cooperation – the Council Framework Decision 2008/977/JHA 27 November 2008.

FRONTEX is allowed to process personal data collected by the member states during joint operations, pilot projects, and rapid interventions of persons "who are suspected, by the relevant authorities of Member States, on reasonable grounds of involvement in cross-border criminal activities, in facilitation of illegal migration activities or in human trafficking activities as defined in Article 1(1)(a) and (b) of Council Directive 2002/90/EC."[150] This data can be used for the preparation of risk analyses, but in the result of these risk-analyses data shall be anonymised.[151] This data can, however, be sent "on a case by case basis" to EUROPOL or "other EU law enforcement agencies." After that the data will be deleted. FRONTEX can keep such data in any case for a maximum of three

144 COM (2010) 584 final, p. 14.
145 Idem, p. 5.
146 Idem, p. 10
147 Idem, p. 11.
148 See in general cooperation between CSDP actors and civilian actors of maritime surveillance: European Defence Agency, Wise Pen Team Final Report of 26 Apr. 2010, pp. 23–27.
149 Recital 7, draft Regulation.
150 Article 11.C.2, FRONTEX Regulation.
151 Article 11.C.3.b, FRONTEX Regulation.

months.[152] It is not clear how the potential surveillance of specific third-country ports and coasts by FRONTEX drones could be squared with this provision, since drones, for example, are likely to be able to process data on *all* persons who find themselves in such an area, including vulnerable groups who might be in need of more protection because they are attempting to flee from persecution. Moreover, as the Spring Conference of European Data Protection Authorities stated in 2008, "the monitoring of travellers has to be well founded and can only be allowed in exceptional cases and for justified and specific purposes. Any general surveillance poses unacceptable risks to the freedom of individuals."[153]

The EUROSUR Regulation should contain a specific provision that explicitly and exhaustively enumerates the conditions under which personal data may be processed in EUROSUR.[154] There is a further need to clarify the provisions regarding the rights of the data subjects, include the right to access personal data that might be collected. While it is encouraging to see a clear prohibition in the proposal on the exchange of information with a third country that could use this information to identify persons, or groups of persons, who are at serious risk of being subjected to torture, inhuman and degrading treatment, punishment, or any other violation of fundamental rights,[155] it remains quite unclear how this provision will be upheld in practice. Since the exchange of EUROSUR information with "neighbouring third countries" would take place on the basis of bilateral or multilateral agreements between the member state(s) and third countries,[156] it would be desirable to mandate the logging of all such information exchanges in order to enable national supervisory authorities to properly review the sending of information to third countries. The EUROSUR Regulation should also include more explicitly a system of layered supervision – with national data protection authorities checking processing of personal data by the National Coordination Centres, and the processing of personal data by FRONTEX, subject to review by the European Data Protection Supervisor (EDPS).

3.1.2 Smart borders

While the exact details of the smart borders initiative are not yet known, the data protection concerns of both systems are relatively straightforward. In this paper we will focus primarily on the data protection concerns related to the EES, since the development of an RTP programme would be highly dependent on the creation of an EES.

Both the EES and RTP envisage the creation of a centralised European database, which potentially includes highly sensitive biometric data such as fingerprints and facial images. According to established case law of the European Court of Human Rights, the mere storing of data amounts to an interference with the right to privacy. The Court has made clear in the *S. and Marper v UK* case that fingerprints and photographs contain unique information that is "capable of affecting the private life

152 Article 11.C.3.a, FRONTEX Regulation.
153 Spring Conference of European Data Protection Authorities, Rome 17–18 Apr. 2008.
154 See also EDPS comments on the proposal for a Regulation of the European Parliament and of the Council establishing the European External Border Surveillance System (EUROSUR) (COM (2011)873 final), 8 Feb. 2012, p. 1.
155 Article 18.2, draft EUROSUR Regulation.
156 Article 18.1, draft EUROSUR Regulation.

of an individual." Retention of this information without the consent of the individual concerned "cannot be regarded as neutral or insignificant," according to the Court.[157]

Persons who want to apply for the RTP would voluntarily enrol by providing immigration authorities with information that goes over and above the information that is required to obtain a visa or enrol as a third-country national not requiring a visa.[158] Persons who consent to have their data processed for this vetting process will need to be informed precisely regarding the exact modalities of the processing and retention of this data in order for them to give their properly informed consent. Third-country nationals who want to enter the EU would have no choice but to allow for the processing of their personal data. The scale of data gathered would clearly need to demonstrate compelling reasons of public safety or public order and should in any case be regulated by a legal framework that includes sufficient safeguards to protect the right to privacy and personal data. At a minimum, the relevant safeguards that are attached to similar databases such as VIS, SIS, and SIS II would need to be applied to an EES/RTP system.

In line with the judgement of the European Court of Justice in the *Huber* case it could be argued that the use of a centralised database which would broadly provide support to border management authorities responsible for the application of the legislation relating to the right of residence is, in principle, legitimate and, having regard to its nature, compatible with the prohibition of discrimination on grounds of nationality laid down by Article 18(1) TFEU. However, such a register must not contain any information other than what is explicitly necessary for that purpose.[159]" Currently the purpose of the EES is not sufficiently clear to meet this standard.

Article 7(e) of the Data Protection Directive provides that personal data may lawfully be processed if "it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed." According to the Commission, the "main purpose" of an EES would be the monitoring of the "respect of the authorised stay of third country nationals (...) as an essential part of first-line risk assessment." The system would also "contribute", to "optimising border check procedures and enhance the security at the moment of the crossing of the external borders".[160] The EES is thus primarily conceived as a migration control instrument that will "increase the numbers of successful returns of irregularly staying third-country nationals."[161] There are, however, major shortcomings with regard to this claim. There are many legal reasons that can explain the overstay of a person and many exceptions in the Schengen Border Code with regard to the registration of entry and exit, so it would be difficult to envisage that an EES alert alone could be the sole basis as grounds for expulsion or deportation. An "overstayers" alert can thus only ever constitute *a presumption* of illegal residence.

If an alert would be triggered immediately when a person has 'overstayed', the system is bound to wrongly identify people who have overstayed for a perfectly legitimate reason. A person may have

157 *S. and Marper v the United Kingdom*, Applications nos. 30562/04 and 30566/04, Judgment, 4 Dec. 2008, para. 84.
158 See also SEC (2008) 153 final, p. 57.
159 Case C-524/06, Heinz Huber v. Bundersrepublic Deutschland.
160 COM (2011) 680 final, p. 4.
161 Idem, p. 11; see also Council doc. 16042/11, p. 27.

started an asylum application or acquired an extended right of residence and failed to exit in accordance with the original entry conditions. "Overstaying" can also be the result of an action beyond a person's control – a stay in hospital due to severe illness, an accident or problem with their scheduled transport, etc. "Alerts" could also result from anomalies in the system: a TCN may have exited and entered through external borders at a place where data has not been collected; a crew member of a plane can cross the border as such, but leave as a normal passenger, and so on.[162] The principle of data-quality[163] requires that every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. It remains to be seen how an EES would be able to address all of these exceptions and requirements.

An entry-exit system could only work when it is infallible, and every entry an exit of every TCN is registered. As the EDPS has noted however, not everybody will be enable to enrol in a programme that uses biometric data. According to the EDPS there are various reasons for this, including as illness, disability, wounds, and burns.

> "It can also in some cases, be linked to ethnicity or occupation. In particular, it seems that a non-trivial number of agricultural and construction workers have fingerprints which are damaged to the point of being unreadable. In other cases, the frequency of which is difficult to evaluate, it may happen that refugees self-mutilate, in order to avoid being fingerprinted.[164]

Given the fallibility of biometric identification systems, and the possibility of system breakdowns[165], "fall back" procedures will be needed in order to allow for the entry of those persons who could not enroll in the system. The Commission argued that the EES would deter TCNs from overstaying, but this claim seems questionnable when there are so many potential loopholes in the system.

It is currently also lawfully impossible to include an EES alert into the SIS/SIS II system, which only provides for the inclusion of deportation orders issued by a court or other competent authority. An administrative procedure must be completed in order to determine whether the person has the right to stay legally in EU territory. Given that there can be no immediate consequences for overstayers following an EES "hit", the extent to which this will lead to more efficient return operations is strongly open to question. Any attempt to automatically link EES alerts to the SIS/SIS II would also likely result in the stopping of an unacceptable number of perfectly innocent travellers. It must also be recalled that border guards already check the passports of departing visa holders for overstays; semi-automating this process will not reduce their workload, it will merely assist them in conducting such checks.

Another purpose of the EES would be that it would be a great source of statistical information on patterns of overstaying (e.g., travel route, fraudulent sponsors, country of origin, and reasons for

162 See in particular the exceptions of Annexes VI and VII of the Schengen Borders Code.
163 See Article 6.1.(d) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
164 EDPS, 2010 EURODAC Opinion, p. 4
165 For a recent example of a biometric database crash see BBC, UK Border Agency ID card system crashes, 3 May 2012, available at http://www.bbc.co.uk/news/uk-17943589

travelling) as well as data on migration flows and overstayers for visa policy purposes.[166] The Danish Presidency's summary of findings of the EU conference on Innovation Border management also stated that a number of participants found that the EES could be "a valuable tool" for detecting, identifying and quantifying overstayers "which can generate valuable information for the purpose of the debate on illegal immigration and support the fight against black market economy, and which can also prove useful for the relation with third countries, e.g. with regard to visa policy." [167] The storage and processing of vast amounts of personal data in such a database, is very unlikely to be necessary within the meaning of Article 7(e) of Directive 95/46. The European Court of Justice has been very clear about this in the Huber case:

> "While Community law has not excluded the power of Member States to adopt measures enabling the national authorities to have an exact knowledge of population movements affecting their territory, the exercise of that power does not, of itself, mean that the collection and storage of individualised personal information is necessary. It is only anonymous information that requires to be processed in order for such an objective to be attained."[168]

The policy development process has introduced a range of other justifications for the EES, including the claim that it could be used to prevent threats against the member states' internal security, specifically for the prevention, detection, and investigation of terrorist and serious organised crimes. This could potentially open the door to the inclusion in the EES of a whole range of data on TCNs not currently subject to a visa requirement that is similar to that collected by the Visa Information System, such as details on fellow travellers (if a person travels in a group), the inclusion of the address of the accommodation provider or place of residence, the final destination, and the purpose of the trip or stay.[169] Some member states have even suggested including information on the vehicles used by TCNs to enter the Schengen area by land, and report on specific categories of objects they carry with them (such as weapons or banknotes). In this instance, it is possible that the police and other internal security services; immigration services; a ministry competent in the field of foreign affairs; authorities dealing with prevention, detection, or prosecution of terrorist crimes; and other serious offences or provincial offices/local authorities that have analogical competences could all be given access to the EES, raising further concerns about data protection and security.

Despite the initial claims of Commissioner Frattini, the Commission itself has already acknowledged that "the potential (of an EES) with respect to reducing terrorism and serious crime is not significant".[170] The Commission notes that "the majority of those refused entries are neither terrorists nor serious criminals but those without the appropriate travel documents and suspected of being prospective illegal immigrants".[171] In theory the EES could provide travel histories of TCNs who are not subject to a visa requirement, including those who are considered "suspects". According to the Commission, "such data on the movements of terrorists and serious criminal suspects could be of value in locating them and in subsequent prosecutions." As Peers notes, "if a person who entered the Schengen territory subsequently was suspected of involvement in a terrorist offence,

166 COM (2008) 69 final, p. 8.
167 Council Doc 7166/12, 2 March 2012 at p. 6. Also, "the EES will be able to provide reliable data, which is otherwise lost as more third countries are granted visa liberalisation."
168 Huber casse at §2.
169 See Article 9, VIS Regulation.
170 SEC (2008) 154 final.
171 SEC (2008) 153 final, p. 9.

the entry-exit system would provide the limited facility of providing information as to whether (and if so, when and where) the suspect has exited the Schengen area, if the suspect has exited that territory legally." [172] This would be the main rationale to retain for a prolonged period of time data of people who left the Schengen area perfectly legal. The gathering of such data seem hard to be squared with the original purpose for which these data were gathered.

Another justification put forward for the creation of the EES is that it could be used to prevent abuses in the area of labour migration, in particular with regard to short stays for work purposes, in which case government agencies dealing with employment and social security might also obtain access to the EES. It is also suggested that the EES could also be used as an anti-corruption measure, as info derived from the EES could be able to identify the border controller at an exact border crossing. This could be used to investigate how unusually large numbers of fake passports get through specific border-crossing points, for instance.

3.1.2.1 The need for safeguards

While we are not convinced that the need for an EES has been demonstrated, we chose to highlight some safeguards that any legislative proposal must contain. As the EES is predominantly an immigration control instrument, routine access for law enforcement authorities (or agencies dealing with employment and social security) to EES data would be unlawful. Firstly, the threshold for internal security authorities to query databases that register "innocent" people should be much higher than the threshold for querying criminal databases. Secondly, such routine access would imply that there is an undeniable link between organised crime and third-country nationals, including asylum applicants and irregular immigrants. As one observer has pointed out: "where no such link has been shown and in the absence of similar measures, including e.g. the centralized storage of sensitive personal information on all EU-citizens, the question remains whether further processing may not even be discriminatory." [173]

The need for access must be demonstrated on a case-by-case basis and show the impossibility – or great difficulty – in obtaining the data by less intrusive means. To enable a review of this principle, a log book could be used to log all uses of EES data by law enforcement authorities. The use of this data must be defined explicitly and restrictively, and go beyond general statements such as "necessary for the performance of their task."

There would also need to be strong data protection provisions setting out the right to information for both applicants to the RTP as well as all TCNs who enter the EU and who will see their data processed in the EES. Information needs to be provided about the identity of the data controller; the purposes for which the data will be processed; the categories of recipients of the data; the data retention period and the existence of the right of access to data relating to them; and the right to request that inaccurate data relating to them be corrected or that unlawfully processed data relating to them be deleted, including the right to receive information on the procedures for exercising those rights and the contact details of the National Supervisory Authorities, which need to be able to hear

172 Peers, "Proposed new border control systems", p. 9.

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) (Dec. 2008): p. 19, available at: http://www.detecter.bham.ac.uk/D14.1BorderControlInternalSecurity-2.doc.

claims concerning the protection of personal data.[174]

A data subject has the right to be informed about the existence of remedies in case his/her application for an RTP has been denied, or when he/she has been classified as an overstayer. There must also be the possibility to appeal or request a review of such decisions before a competent judicial or administrative authority, or a competent body composed of members who are impartial , who enjoy safeguards of independence in the Member State issuing the 'overstayers alert', and who are competent to judge the proportionality and the lawfulness of the measure..[175] Article 22 of the EU Data Protection Directive states very clearly that "every person" has a right to a judicial remedy, irrespective of his place of residence – this right applies to TCNs as well.

As stated above, stringent data quality requirements are essential because EES data could be used for a range of purposes that might be prejudicial to the interests of the data subject. The European Commission has acknowledged that this is a "potential problem, as with any data of this type, that it could be used inappropriately."[176] Legal provisions will need to be adopted that allow for third-country nationals to enter, even if they were not able to enrol in a programme that uses biometric data.[177]

3.2 Interference with the right to asylum

Both the EES and EUROSUR can have a negative impact on refugees and potential applicants for asylum. The EDPS has stressed the indirect effect of border-control measures, stating that they "may deter people to seek the protection they are entitled to in Europe under international rules of protection of refugees."[178] Indeed, the demand for EUROSUR and smart borders builds on a longer-term trend in EU policy that makes it increasingly more difficult for refugees and others in need of protection to reach EU territory. It is clear that the purpose of both systems is to extend EU border surveillance further away from the EU's actual territorial borders into the high seas and territories of third countries ("the pre-frontier area"). This trend can only be interpreted as a concerted attempt by the member states to avoid responsibility for asylum claims. While neither system can legally affect the obligations of member states under Article 18 of the Charter of Fundamental Rights and the 1951 Convention relating to the Status of Refugees,[179] specific safeguards must be included to ensure that refugees bound for Europe can access a procedure.

174 See similarly Articles 37–38 of the VIS Regulation.

175 SEC (2008) 153 final, p. 58. See also article 40, VIS Regulation. See also the related recommendation of the Meijers Committee on article 43 of the amended SIS II Regulation, p.7, "2. Any person may bring an action before the courts or the authority competent under the law of any Member State to access, correct, or delete or obtain information or to obtain compensation in connection with an alert relating to him. 3. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraphs 1 and 2, without prejudice to the provisions of Article 48. 4. The rules on remedies provided for in this Article shall be evaluated by the Commission by […]."

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

177 EDPS, VIS Opinion, OJ C 181/19.

178 EDPS, 2008 Opinion prelim., p. 6.

179 Recital 16 to the draft EUROSUR Regulation explicitly states that "the implementation of this regulation (…) does not affect obligations of Member States under the United Nations Convention on the Law of the Sea, the International Convention for the Safety of Life at Sea, the International Convention on Maritime Search and Rescue, the United Nations Convention against Transnational Organised Crime and its Protocol against the

3.2.1 EUROSUR

EUROSUR has an ambiguous relation with the right to asylum. The Commission's proposal mentions that within EUROSUR's scope, member states and FRONTEX shall give special attention to "victims of trafficking, persons in need of urgent medical assistance, persons in need of international protection, persons in distress at sea and other persons in a particularly vulnerable situation."[180] In its earlier Communications, the Commission has repeatedly stressed that one of the primary reasons for the establishment of EUROSUR is that it would enable the saving of lives at sea. The early detection of small, unseaworthy boats that are overcrowded and without any safety equipment or illumination would enable an intervention by FRONTEX or a member state, which would prevent lives lost at sea.[181]

EUROSUR is presented as reinforcing the search and rescue capabilities of member states to "ensure that as many persons as possible are brought to safety."[182] The support to such search and rescue missions is "without prejudice to the functions and tasks of the responsible Rescue Coordination Centres."[183] The EU Fundamental Rights Agency has also argued that "best use should be made of the live-saving potential of the EUROSUR system," which can provide early information on vessels or persons threatened by grave and imminent danger requiring immediate assistance.[184] While we agree with the Fundamental Rights Agency, we are concerned that without specific rules on the primacy of search and rescue functions, this potential may not be realised. EUROSUR could clearly help to bring more people to "safety", but nowhere in the proposal is it defined how exactly this will be done, nor are there any procedures laid out for what to do with the "rescued". These boats typically contain irregular migrants and persons in need of international protection, but nothing is said about the need to process a request for asylum of the latter group. Conversely, Article 2.2 of the proposed Regulation states that the EUROSUR Regulation shall "not apply to operational, procedural and legal measures taken after interception." The impact assessment is even more explicit, stating that "asylum, readmission, and return" are out of the scope of EUROSUR.[185]

If the EU harbours genuine ambitions to save lives at sea, it must at least specify how EUROSUR will send information or alerts to the Rescue Coordination Centres of the country responsible for a specific search and rescue region. In this context it should be noted that the 2010 amendment of the Schengen Border Code already includes such a provision in its non-binding annex on "Guidelines for search and rescue situations and for disembarkation in the context of sea border operations".[186] A

Smuggling of Migrants by Land, Sea and Air, the Convention relating to the Status of Refugees, the Convention for the Protection of Human Rights and Fundamental Freedoms and other relevant international instruments." A similar clause would be needed in the EES proposal.

180 Article 2.3, draft EUROSUR Regulation.

181 See also (SEC (2011) 1536 final, p. 9, and Parliamentary Question, E-006760/2011; answer given by Ms Malmström on behalf of the Commission (28 July 2011).

182 Idem.

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

184 Fundamental Rights Agency, The Stockholm Programme: A chance to put fundamental rights protection right in the centre of the European Agenda, Vienna, 14 June 2009, p. 8.

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

186 Article 1.2 of this annex explicitly states that "when facing in the course of the border surveillance operation a situation in which uncertainty or apprehension exists as to the safety of a ship or of any person on board, the participating unit should forward as soon as possible all available information to the Rescue Coordination Centre responsible for the search and rescue region where the situation is taking place."

more fundamental point needs to be stressed here as well, particularly in the light of the recent 'Hirsi' judgment on the illegality of Italian "push-back" operations to Libya.[187] States cannot simply circumvent refugee law and human rights requirements by equating interception measures on the high seas to prevent migrants from reaching Europe's borders with search and rescue measures, as is the case in the current guidelines for joint operations. But without strict guidance for FRONTEX and the member states, the default position is almost certain to remain in practice a preference for interception and *refoulement* over rescue and refugee protection.

The Technical Study illustrates this dilemma with an example of the kind of "operational information" EUROSUR's Common Pre-frontier Intelligence Picture will provide:

> 5th May 20XY: According to satellite imagery provided by XY, this morning around 5am 7 wooden boats (length 12-15m) with about 250 illegal migrants departed from the coast of the African country Z next to the village K (coordinates xz East yw West) in harsh weather conditions (wind level 5 increasing). The type of boats used has typical speed of 7-8 knots. Due to the current migration trends, it is expected that the boats will head for MS A (70% probability) or for MS B (30% probability). The authorities of country Z have been contacted by NCC A, which, despite the recently delivered patrol boats, is not expected to take any action. NCC A is currently coordinating with NCC B and FRONTEX (joint operation Karies) their patrolling activities for SAR and interception. FRONTEX is currently redirecting satellites and two surveillance planes over the area TOMATO (route to MS A).[188]

Despite the "harsh weather conditions" and likelihood of overcrowding in the boats, it is far from clear from this example that the goal of the alert and subsequent surveillance measures is *a priori* to save lives, in spite of the obligation on holders of such information stemming from the SOLAS Convention, to prioritise any such assistance that can be given. The current lack of detail on EUROSUR's aim of "rescuing lives at sea" in the draft EUROSUR Regulation – coupled with a high level of detail on the border-control capacities of the system – means that it is essential to amend the draft Regulation so that search and rescue obligations are both strengthened and read jointly with the requirements of refugee law and human rights law.[189] The likely annulment of the aforementioned Guidelines for joint operations gives the European Parliament the chance to demand a coherent policy that is reflected in both policy and practice.

3.2.2 Entry-exit system

As noted above, in regard to the EES, further safeguards are needed because there may be justified reasons for an "alien" to "overstay", or instances where the system will wrongly identify people as having done so. S/he may have started an asylum application or acquired an extended right of residence and failed to exit in accordance with the original entry conditions. It is therefore

187 *Hirsi and others v Italy*, case no. 27765/09.

188 Subproject 3, Final report – Common Pre-frontier Intelligence Picture, "Technical and management concepts for the surveillance of land and maritime borders", Technical Study for the European Commission Directorate-General for Justice, Freedom and Security, Within the Framework of a European External Border Surveillance System (EUROSUR), January 2010, p. 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): p. 199. "Member states and FRONTEX cannot intercept migrants as a means to reduce loss of life without considering the need to avoid disembarkation in territories where the lives and freedoms of those alleging a well-founded fear of persecution or as a real risk of ill treatment may be put in jeopardy."

imperative that any future EES legislation stipulates that any "overstay" alert can only ever constitute a *presumption* of illegal residence. Once an alert has been issued, a proper procedure must be completed in order to determine whether the person has the right to stay legally in EU territory. This procedure must give the traveller the chance to explain the circumstances of any "overstay". An EES alert alone can never be grounds to refuse entry or to deport a person and should not therefore be included in the Schengen Information System.[190] In fact, it is quite unclear how any kind of automatic sanction could be attached to an EES alert. To confirm, the scope and function of the EES must therefore be limited to border officers carrying out checks on passengers, and files should only be kept in the EES after a person has exited the EU if the assumption of an illegal stay is confirmed.

190 The Returns Directive provides for sanctions in cases of illegal residence or overstayers, including a returns decision (which includes a period for voluntary departure and a re-entry ban) and coercive measures to carry out the removal of a TCN.

4 Cost, necessity, and effectiveness

The cost of implementing the EUROSUR system during the period 2011–2020 is estimated at €340 million. The European Commission has set aside a further €1.1 billion to fund the smart borders initiative (Entry-Exit System and Registered Traveller Programme) from the proposed Internal Security Fund (ISF) 2014–2020. A full policy impact regarding the proposed EUROSUR and planned EES and RTP is well beyond the scope of this report. Instead we make some observations about the feasibility studies and cost estimates that have been produced during the EU policy-making process. We also examine EU-funded research and development (R&D) in support of the three proposed systems from the EU's €53.2 billion Seventh Framework Programme for Research and Technological Development (FP7, 2007–2013) and outline the way the EU's External Borders Fund, Development Cooperation Instrument, and ISF have been used, or will be used, to pay for the implementation of EUROSUR, EES, and RTP in member states and third countries. Finally, we suggest that it might be instructive for the European Commission to re-assess its proposals in light of the United States' experience in attempting to develop and implement similar systems.

4.1 Feasibility studies and cost estimates

The potential impact on the fundamental rights to privacy and data protection means the EUROSUR, EES, and RTP proposals should be subject to a "necessity test". The European Court of Human Rights has held that interference with a right is seen as "necessary" if it answers a pressing social need, if it is proportionate to the aim pursued, and if the reasons put forward by the public authority to justify it are relevant and sufficient.[191] New information management systems in particular need to be accompanied by "clear proof of their necessity and proportionality"; such proof should be provided by a privacy impact assessment based on "sufficient evidence".[192] As the European Commission has acknowledged, "being useful is not sufficient to justify the implementation of systems like an EES and a RTP."[193] Nevertheless, the European Data Protection Supervisor has criticised the Commission's general approach to impact assessments for failing to consider "concrete measures and mechanisms which would ensure that both necessity and proportionality are respected and

191 *Handyside v United Kingdom*, (App. N° 5493/72), 7 Dec. 1976, § 48. The notion of necessity implies a stricter burden of proof than just being "useful". The European Court of Human Rights has held on numerous occasions that while the adjective "necessary" is not synonymous with "indispensable", it has neither the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable", or "desirable".

192 EDPS, July 2010, p. 7. These could either take the form of a separate privacy and data protection impact assessment or be integrated into the general impact assessment. The current guidance on impact assessments (European Commission Impact Assessment Guidelines, SEC (2009) 92) does not foresee a separate impact assessment for the impact on fundamental rights, such as data protection; these aspects are to be integrated in the general impact assessment. In the meantime, following the Commission's Communication on the strategy for the effective implementation of the Charter of Fundamental Rights by the European Union (COM (2010) 573), additional guidance has been prepared in the form of a Commission Staff Working Paper on operational guidance on taking account of Fundamental Rights in Commission Impact Assessments (SEC (2011) 567).

193 COM (2011) 680 final, p. 11.

practically implemented in all proposals having impact on individuals' rights."[194] No meaningful fundamental rights or privacy impact assessment was carried out for EUROSUR on the grounds that personal data will not be routinely processed by the system, though the impact assessments did recognise the need for fair and lawful processing for explicit and legitimate purposes.[195] With regard to EES, the European Commission has yet to explain how the "significant human rights impact" identified in the 2004 impact assessment has been overcome.[196]

4.1.1 EUROSUR

Various studies and assessments were produced prior to the EUROSUR proposal of December 2011. A feasibility study – the BORTEC study produced by FRONTEX – was completed in 2007. A roadmap to implement the EUROSUR system was then produced by the European Commission in 2008, accompanied by an impact assessment. A further Technical Study setting out the management procedures for EUROSUR and the operational requirements for the Communication system and the Common Pre-Frontier Intelligence Picture was produced by a contractor in 2010, at a cost of €1.8 million. A second impact assessment was then produced by the Commission to accompany the 2011 legislative proposal. A EUROSUR Financial Study was commissioned to support the second impact assessment. We are concerned that this process has not allowed for adequate democratic control or impartial assessment of the merits of the EUROSUR proposal.

Feasibility studies are supposed to objectively and rationally uncover the strengths and weaknesses of a proposed course of action, the risks it faces, and ultimately the prospects for success. The BORTEC feasibility study, which was given the mandate of designing a basic framework for EUROSUR, did not meet this standard. The decision to begin developing the system in 2008 then pre-judged any further impact assessment. As the Commission noted in its 2011 assessment, "While the impact assessment presented in 2008 assessed the different components proposed in Steps 1 to 7 of the EUROSUR roadmap, thereby identifying *'what'* should be done, the current impact assessment assesses *'how'* these components should be implemented until 2013 on the basis of the works carried out between 2008 and 2011."[197] Thus, whereas the 2008 impact assessment presented the decision to establish EUROSUR as one of the necessities to achieve more effective border control (this was essentially a choice between total border control, advanced/smart border control, or no border control), the 2011 impact assessments simply offered three different policy options and cost estimates for implementing the system. The sheer scale of deaths in the Mediterranean of migrants and refugees bound for Europe alone[198] provides an overwhelming case for establishing a system capable of saving lives at sea. But as noted above, in the absence of detailed guidance on how lives will actually be saved by EUROSUR (beyond identifying the vulnerable), it is difficult to assess its potential.

194 EDPS 2010 opinion on overview of information management systems, p. 7
195 SEC (2011) 1536 final, p. 32.
196 European Policy Evaluation Consortium, "Study for the extended impact assessment of Visa Information System", Dec. 2004, pp. 31–37.
197 SEC (2011) 1536 final, p. 5 [emphasis in original].
198 See "Death by policy: The fatal realities of 'Fortress Europe' – 15181 deaths", available at: http://www.unitedagainstracism.org/pages/campfatalrealities.htm.

We are also concerned that the prospects of EUROSUR achieving its key operational objective (continuous surveillance of the wide areas of open seas in order to detect and track small vessels from the point they depart the territorial waters of a third state) have not been subject to impartial scrutiny or review. As the BORTEC study noted, "although it is theoretically possible to carry out the surveillance of all areas of the Open Sea 24/7, it would need an unbearable amount of resources without really knowing the outcome of such endeavour."[199] Instead of clearly demonstrating the technical capacity of the proposed EUROSUR system, the European Commission has simply drafted the legislation broadly enough to encompass any solution that may be found, while outsourcing the research and development to the European Security Research Programme (see section 4.2).

The EUROSUR Technical Study produced in 2010 by German defence contractor ESG and subcontractors EADS, SELEX-Finmeccanica, and Thales lists 11 types of "surveillance sensors" and 18 types of "maritime surveillance" systems that *could* be used for the surveillance of land and maritime borders.[200] These are among the 13 different sources of information that will contribute to the national and European situational pictures. We are concerned that the sheer scope of the planned system is a potential recipe for technical failures and cost overruns. It is also regrettable that both the BORTEC and ESG studies have been withheld from the European and national parliaments and wider public scrutiny.

Despite mandating the technical development of EUROSUR in 2008, the European Commission did not begin to assess the potential costs until 2011, when it commissioned a "Technical Study assessing the financial impact of establishing the European Border Surveillance System" to consultants GHK, Unysis, and EUROCONSULT.[201] The study was required to provide cost estimates for three options for establishing EUROSUR over the period 2011–2020: (i) a decentralised approach to EUROSUR based on interlinking member states only; (i) a partly centralised approach with some data centralised at FRONTEX; or (iii) a fully centralised approach. The estimates, which do not include annual operating costs, ranged from €318 million for a decentralised EUROSUR up to €913 million for a fully centralised system. The preferred option is the "partly-centralised approach", estimated at €338.7 million (see Figure 4).[202]

The estimated costs were themselves based on earlier estimates provided by the EUROSUR Technical Study, member state responses to a questionnaire, and actual projects supported by the European Border Fund. A quarter of the member states failed to provide any financial data at all, and among those that did, "the completeness and comparability of that data varied to a large extent."[203] So in estimating the costs of upgrading the National Coordination Centres and integrating FRONTEX into EUROSUR (see Figure 5), the contractors simply took one or two "reference states" for each policy option and extrapolated a total figure based on national and FRONTEX estimates.[204] The European Commission should have acknowledged that the margin of error of such an approach

199 BORTEC Study, p. 98.
200 Subproject 1, "Technical and management concepts for the surveillance of land and maritime borders", Technical Study for the European Commission Directorate-General for Justice, Freedom and Security, Within the Framework of a European External Border Surveillance System (EUROSUR), January 2010.
201 Technical study assessing the financial impact of establishing the European External Border Surveillance System (EUROSUR), Final Report, Directorate-General for Home Affairs, September 2011.
202 SEC (2011) 1536 final, p. 38–39.
203 SEC (2011) 1536 final, p. 36.
204 Belgium and France were used for Option 1, Slovakia and Cyprus for Option 2, and Finland for Option 3.

renders its estimates as purely speculative. Funding the development and implementation of EUROSUR from the European Security Research Programme and External Border Funds, respectively, will add to the already existing difficulties in monitoring expenditure and detecting cost overruns or bad investments.

Figure 4: "Policy options" for funding EUROSUR[205]

Step	Component	Option x.1	Option x.2	Option x.3	Preferred options	
		Decentralised approach	Partly centralised approach	Centralised approach	Respon-sible	Funding
1	National coordination centres	M€ 99,6	M€ 271,6	M€ 610	Member States	EBF (ISF)
1	Frontex Situation Centre	M€ 95,6	M€ 129,8	M€ 137	Frontex	Frontex (ISF)
2, 7	Communication network	M€ 42,4	M€ 46,7	M€ 49,3		
6	Common Pre-Frontier Intelligence Picture	€ 0,0	M€ 29,3	M€ 29,2		
3	Networks with 3rd countries	€ 0,0	M€ 5,4	M€ 25,3	Member States	DCI, EBF (ISF)
5	Common application of surveillance tools	M€ 80,5	M€ 62,1	M€ 62,3	Frontex EUSC EMSA	Frontex GMES
Total		M€ 318,1	M€ 544,9	M€ 913	Legislative finan-cial statement: M€ 244 (2014-20)	
Preferred Option		M€ 338,7 (2011-2020)				

Figure 5: Estimated EUROSUR costs: National Coordination Centres and FRONTEX[206]

Cost comparison between policy options, 2011-2020. Euros (€) and per cent (%)

	Baseline (2007-2010)	Policy 0ption 1.1: Decentralised Option (2011-2020)	Policy 0ption 1.2: Comprehensive option (2011-2020)	Policy option 1.3: Centralised option (2011-2020)
Total costs NCC	€40,054,849	€99,697,200	€271,673,160	€610,386,216
Total costs FSC	€2,238,499	€95,591,020	€129,824,552	€136,983,844
TOTAL COSTS	**€42,293,348**	**€195,288,220**	**€401,497,712**	**€747,370,060**
MS share (%)	95%	51%	68%	82%
FSC share (%)	5%	49%	32%	18%

205 Source: SEC (2011) 1536 final, p. 39.
206 Idem, p. 31.

4.1.2 Entry-Exit System and Registered Traveller Programme

In 2008 the European Commission suggested that the "estimated costs of the centralised entry/exit and Registered Traveller Programme system would be approximately 20 million euro, spread out over 2-3 years and the annual maintenance and operational costs approximately 6 million euro."[207] It estimated that it would cost a further €35 million to implement the EES and RTP in the member states, "but [this] could vary greatly depending on the number of automated gates that would be implemented. One automated gate unit costs approximately 35,000 euro."[208] The Commission justified its modest estimates on the grounds that neither system would be as expensive as the Visa Information System, "since the technical design of both should allow for maximum synergies with the VIS."[209] But as Peers noted, this estimate apparently failed to take into the account the cost of using or upgrading VIS to record the exit of TCNs at external borders.[210] When the Commission revisited the potential costs of the EES and RTP in 2011, its estimates increased dramatically: The development of the central EES and RTP could be in the order of €400 million, with annual operating costs of €180 million per year for the first five years. If the EES and RTP were built on a single technical platform, the Commission estimated a cost saving of up to 30 per cent.[211] The Commission has allocated €1.1 billion to the development and implementation of these systems from the proposed EU ISF 2014–2020 (see section 4.3.3).

The substantial costs of developing the EES can only be justified on the basis of a clear demonstration of their necessity and proportionality. With regard to the Entry-Exit System, it has not yet been demonstrated that it will prove useful in preventing and detecting people who overstay their visas. As noted above, this objective *might* be met if EES overstays were linked to police alerts via the SIS/SIS II, but this is currently unlawful (any amendment of the SIS rules would also require a clear demonstration of proof of the necessity and effectiveness). The value of EES as a security measure is even more doubtful. An EU Action Plan on Combating Terrorism from 2006 included an automated Entry-Exit System among the border control measures that "could" be taken to prevent

207 The Commission would be responsible for acquisition and maintenance of the central database (the centralised EES and RTP database), while member states would be responsible for arranging equipment such as fingerprint readers, equipment to store the biometric identifiers, potential (semi-) automated border checks, separate lanes etc., as well any equipment/staff needed for enrolment of registered travellers as such. SEC (2008) 153, pp. 27, 30.

208 SEC (2008) 154.

209 SEC (2008) 153, p. 20. In 2004 the question of setting up an automated EES at the external borders of the EU was addressed in the framework for the Impact Assessment for setting up the VIS. In that context, the view was taken that the EES would have been "too costly and disproportionate", SEC (2008) 153, p. 24.

210 Peers notes that "in the absence of an obligation to use the current VIS on exit, it is possible that some Member States may not install the infrastructure to use the VIS at some exit points. If that is the case, the Commission's assumed status quo would again fail to assess fully the costs of introducing an entry-exit system, since there would be an obligation upon Member States to install infrastructure at all exit points in order to ensure the full functioning of the system." Steve Peers, "Proposed new border control systems", Briefing Paper for the European Parliament, PE 408.296, 25 June 2008.

211 COM (2011) 680 final, p. 10 (based on a study carried out for the Commission in 2010).

terrorism,[212] but the European Commission has already recognised that "the potential (of an EES) with respect to reducing terrorism and serious crime is not significant".[213]

Figure 6: Estimated costs of the RTP and EES systems by the Commission[214]

	One-time development cost at central and national level (3 years of development) (in EUR million)	Yearly operational cost at central and national level (5 years of operation) (in EUR million)	**Total costs at central and national level** (in EUR million)
RTP: Option – Data (unique number) stored in a token and (biometrics and data from applications) in a repository	207 (MS- 164 – Central- 43)	101 (MS- 81 – Central- 20)	**712**
EES: Option – Centralised system with biometrics added later	183 (MS- 146 – Central- 37)	88 (MS- 74 – Central- 14)	**623**

It is also obvious that an EES could also result in significantly increased waiting lines for third-country nationals wanting to enter the Schengen area. Whereas TCNs subject to a visa requirement are already required to provide biometric data on entry, those on the so-called "white lists", who do not require an advance visa, are exempt from this requirement. Extrapolating from border-crossing statistics collected during a comprehensive monitoring exercise in 2009 [215], this could result in the fingerprinting of an additional 57 million "white list" TCNs. The VIS impact assessment of 2004 stated that on average 15 seconds were added to entry procedures in the United States when biometrics were collected for the United States' US VISIT programme. If the EU were able to achieve this target

212 Council doc. 5771, 27 Jan. 2006.

213 SEC (2008) 154 final. The Commission notes that "the majority of those refused entries are neither terrorists nor serious criminals but those without the appropriate travel documents and suspected of being prospective illegal immigrants", SEC (2008) 153 final, p. 9. In theory the EES could provide travel histories of TCNs who are not subject to a visa requirement, including those who are considered "suspects". According to the Commission, "such data on the movements of terrorists and serious criminal suspects could be of value in locating them and in subsequent prosecutions." As Peers notes, "if a person who entered the Schengen territory subsequently was suspected of involvement in a terrorist offence, the entry-exit system would provide the limited facility of providing information as to whether (and if so, when and where) the suspect has exited the Schengen area, if the suspect has exited that territory legally." Peers, "Proposed new border control systems", p. 9.

214 COM (2011) 680 final, p. 14.

215 Council Doc. 13267/09, 22 September 2009.

with regard to 57 million TCNs, it would add the equivalent 27 years of queuing time per year at the EU borders. As noted above, adequate provision would also have to be taken for false positives, failures to provide biometrics, and a range of other eventualities.

The European Commission has argued that the "substantial costs foreseen at this stage need to be considered alongside the benefits: for example, together with automating a substantial share of all border crossings, the RTP could reduce border control resources needed by around 40% (equivalent to EUR 500 million/year). Even if the calculation is based on more modest savings of EUR 250 million/year, Member States could have net cost savings already after the second year of operation."[216] No details are provided of how these cost savings are to be achieved beyond the implied reduction in staff required because of the use of automated gates. Moreover, while a voluntary EU-wide RTP programme might enable registered travellers to cross borders much faster than their unregistered counterparts, the Commission has estimated that only 4 to 5 million travellers per year might actually use it.[217] Estimates suggest that this amounts to no more than five per cent of TCNs crossing external borders annually. Since the shorter queues at RTP gates seen to date are the result of relatively few people being a part of such programmes (which typically charge an annual fee of around €125), there must be significant doubts as to their capacity to relieve the pressure on Schengen borders or facilitate travel for the vast majority.[218] The rationale for automated border control gates might be strengthened if their use was mandatory for all travellers, including EU citizens, but this far exceeds the scope of the envisaged proposals.

4.2 Border security and the European Security Research Programme

The increasing emphasis on the use of new technologies in support of EU border control policy has correlated closely with new approaches to 'border security' being developed as part of the European Security Research Programme (ESRP). The ESRP was launched in 2004 and then integrated into the EU's Framework Research Programme, 'FP7', which runs from 2007-2013.[219] The ESRP has the twin objectives of enhancing the security of European citizens and supporting the development of a globally competitive security industry in Europe.[220] The European Commission has increasingly used the ESRP to fund projects in support of the technological development of the EUROSUR system. Further projects have showcased the technologies behind smart borders and the development of systems used for "profiling" the travelling public.

Border security is one of ESRP's five core "mission areas" and has been at the heart of the programme since its inception. In October 2004, the European Commission held a workshop in Ljubljana (Slovenia) on "Research and Technological challenges in the field of Border Control", bringing together EU policy-makers, national border guards, and some of Europe's largest defence companies, including Finmeccanica, Thales, EADS, Sagem, and the AeroSpace and Defence Industries Association of Europe (a lobby group representing Europe's largest alliance of security and defence

216 COM (2011) 680 final, p. 10.
217 COM (2011) 680 final, p. 12.
218 SEC (2008) 153, p. 66.
219 Decision 2004/213/EC of 3 February 2004 on the Preparatory Action for Security Research; Decision 1982/2006/EC of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013).
220. Annex 1, Decision 1982/2006/EC.

contractors). These companies were also represented on the successive advisory groups established by the European Commission to advise the EU on the ESRP, notably the "Group of Personalities" and the European Security Research Advisory Board, whose joint chairs were the directors of Thales and EADS.[221] The Board's final report of September 2006 set the priorities for the "security" component of the FP7 programme.[222]

In the area of "border security", these were defined as "detection, identification and authentication" technologies, "situation awareness and assessment, including surveillance", information management, communication, training and exercises. Within these priority areas, five research domains were identified: port security (including containers), sea borders surveillance, unregulated land borders, checkpoints, and "extended smart borders".[223] Figure 7 from the Board's report provides an illustrative summary of the R&D priorities of the FP7's "border security" component. A third European Security Research Advisory Board, the "European Security Research and Innovation Forum", was established in early 2007, with a mandate to develop a 20-year vision for the ESRP. European Security Research and Innovation Forum Working Group 3 focussed on "border security".[224] It was chaired by Erik Berglund, then head of FRONTEX's Research and Development Unit, with Giovanni Barontini, then Vice President of Italian defence giant Finmeccanica's civil applications division, appointed as Rapporteur. The final European Security Research and Innovation Forum report described the two key challenges for the ESRP in supporting the EU's policy on integrated border management and making the requisite technical equipment affordable enough to be widely employed.

Erik Berglund, now FRONTEX's Director of Capacity Building, has spoken frankly about the importance of engaging with the ESRP. "We [FRONTEX] needed to occupy some ground in the external world if we were to be effective. And the big opportunity at that time was to get into the EU security research which had just restarted in earnest that year."[225] The FRONTEX Research and Development Unit was soon participating in evaluation of FP7 research project proposals and found itself represented on the end-user advisory boards, "where it could exert useful influence on [project] development". The agency now holds seminars with technology suppliers at least twice a year to ensure that the security industry is able to showcase its latest products while industry representatives from selected projects regularly participate in the FRONTEX-chaired FP7 Implementation Group on maritime border surveillance. FRONTEX is also represented on the 20 member Security Advisory Group (SAG), which advises the European Commission on the annual calls for proposals for the European Security Research Programme.[226] Like other observers, we are concerned that the ESRP appears to have had the effect of consolidating relations between the security and defence industries and those responsible for developing and implementing border security policies at the EU level, while at the same time marginalising those perspectives that are not

221 Hayes, "Neoconopticon: The EU security-industrial complex", *TNI/Statewatch* (2009): pp. 15–17.
222 "Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board", Brussels: European Commission, 2006.
223 European Security Research Advisory Board report, p. 25.
224 "European security research and innovation forum", Final Report, Brussels: European Commission, 2009.
225 FRONTEX (2010) "Beyond the Frontiers - Frontex: The First Five Years", p. 53, available at: http://www.frontex.europa.eu/assets/Publications/General/Beyond_the_Frontiers.pdf.
226 The security industry is also well represented on the SAG, see current membership, available at: http://ec.europa.eu/research/fp7/pdf/advisory-groups/security-members.pdf#view=fit&pagemode=none.

convinced of the need for smart surveillance or smart borders.[227] As a study commissioned by the European Parliament's 'Citizens' Rights and Constitutional Affairs' policy department found in November 2010:

> EU security research and development activities have been mainly driven by a concern to bring together representatives from the ministries of Defence and Interior of the Member States and Associate countries, and representatives of major companies from the defence and security industries. In the process, representatives from civil society and parliamentarians, as well as bodies and organisations in charge of civil liberties and fundamental freedoms, including data protection authorities and fundamental rights bodies, have been largely sidestepped. The outcome of this process is a dialogue that is limited in its scope, addressing security research through the concerns of security agencies and services and the industry, without taking into account the requirements flowing from the EU's internal area of freedom.[228]

227 Bigo and Jeandesboz, "The EU and the European security industry: Questioning the 'Public-Private Dialogue'", INEX Policy Briefs no 5, CEPS, 2010; Burgess and Hanssen, "Public-private dialogue in security research", Brussels: European Parliament, PE 393.286, 2008.

229 "Review of security measures in the Research Framework Programme", Brussels: European Parliament Directorate General for Internal Policies, 2010, p. 10.

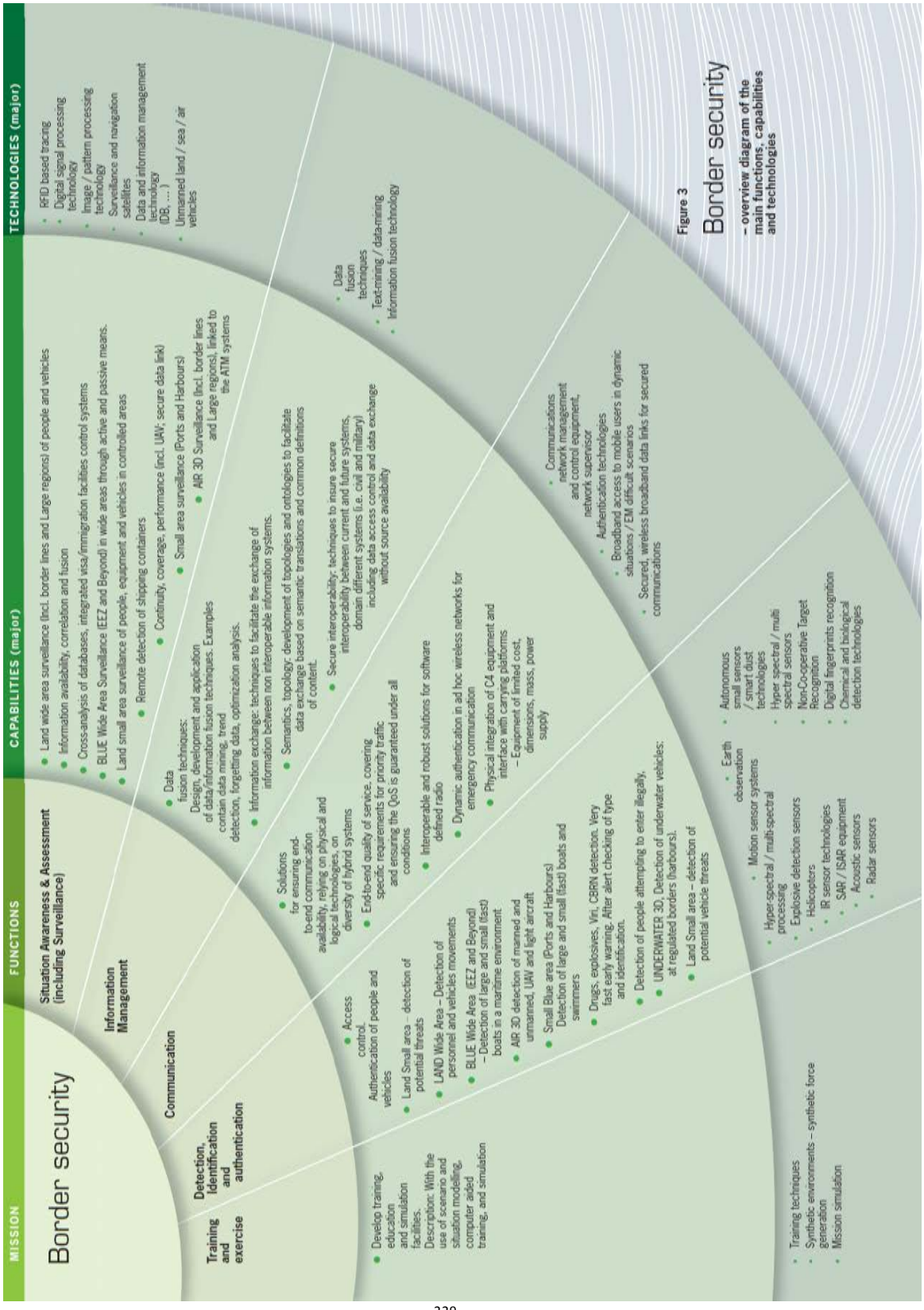


Figure 7: Achieving border security in the EU[229]

4.2.1 EU funded R&D projects supporting EUROSUR

Research, development, and testing of EUROSUR components and shared surveillance tools has been outsourced to the European Security Research Programme, which has been used to fund studies, R&D, and demonstration projects on border surveillance and control. Draft EU legislation

229 European Security Research Advisory Board report, p. 26.

establishing the Eighth Framework Programme on RTD ("Horizon 2020", 2014–2020) would formalise this process by including R&D in support of EUROSUR as an explicit priority of the ESRP.[230] Horizon 2020 is "aimed at securing Europe's global competitiveness", "part of the drive to create new growth and jobs in Europe" by creating an "Innovation Union".[231] Some may question, however, whether this programme is the appropriate instrument from which to fund R&D into the development of EU border controls.

Box 4 details 15 projects funded to date in the area of border security to which the EU has contributed more than €170 million. More than half have provided indirect or direct input to the development and implementation of EUROSUR. Before the current framework research comes to an end in 2013, the results of two more calls for border surveillance proposals will be announced. In the 2011 call, the EU requested proposals on "Increasing trustworthiness of vessel reporting systems" and the "Pre-Operational Validation (POV) at EU level of common application of Surveillance tools".[232] The forthcoming 2012 call will include the "Surveillance of wide zones: from detection to alert"; "Pre Operational Validation on land borders"; "Sensor technology for under foliage detection"; and "Mobile equipment at the land border crossing points".[233] If Horizon 2020 is used to fund EUROSUR-related R&D at the current rate that the European Security Research Programme is being used, then the investment between now and 2020 could be in the region of €300–400 million, dwarfing the estimates provided by the Commission.

While it is logical for the EU to conduct R&D in support of its policy objectives, a separate budget line for EUROSUR R&D with clear goals and objectives would provide for greater democratic control and accountability. We are also concerned that the main recipients of this R&D funding to date have been large defence and security companies that stand to profit if the member states or EU agencies make subsequent investments in the border surveillance technologies they promote. Eleven out of the 13 projects described below are/were led by defence contractors (see Box 4). All seven of the projects detailed in the following sub-section are/were also led by large defence companies. The majority of the consortia participants are from the defence sector. The same names – whose influence on the framework research programme is well-documented – are omnipresent.

A potential conflict of interests hangs over the evident outsourcing of the design, development, and implementation of the EUROSUR system to date (see Box 4). This process is also clearly encouraging the transfer of applications developed in the military sector into the (traditionally) civilian realm of border control and maritime surveillance, raising questions about the legitimacy of funding apparently "dual use" research and impacting significantly on the way that migration is perceived and policed. It is striking that whereas EUROSUR has the triple objectives of preventing illegal migration, combating transnational crime, and saving lives at sea, the EU has neither funded nor called for proposals geared solely towards safety or search and rescue. Finally, whereas all of this R&D must be "state-of-the-art" in order to qualify for EU research funds, there has been no meaningful independent review of the results of the projects detailed below with regard to their implications for the development of EUROSUR or the viability of specific technologies.

230 EU Council doc. 17935/11, p. 81.
231 See Horizon 2020, available at: http://ec.europa.eu/research/horizon2020/index_en.cfm?pg=h2020.
232 FP7-SEC-2011-1, 20 July 2010.
233 FP7-SEC-2012-1 Orientation Paper, 17 Apr. 2012.

Box 4: EU security research projects supporting EUROSUR

Project name	Objective	Start date	Dur-ation	Cost (EU contrib -ution)	Led by
PERSEUS (Protection of European seas and borders through the intelligent use of surveillance)[234]	(1) Showcase an "EU Maritime Surveillance System of Systems" incorporating "existing national systems and platforms, enhancing them with innovative capabilities and moving beyond EUROSUR's 2013 expectations"; (2) support the development of the member states' NCC network and incorporate both FRONTEX and the surveillance systems of the European Maritime Safety Association. Includes applications to improve "detection and identification of non collaborative/suspicious small boats and low flying aircraft"; "enhanced and increasingly automated detection of abnormal vessel behaviours"; and "identification of threats and tracking of reporting and non-reporting vessels".	Jan. 2011	4 years	€43.7m (€27.9m)	Indra Sistemas
SEABILLA (Sea Border Surveillance)[235]	(1) Define the architecture for cost-effective European Sea Border Surveillance systems, integrating space, land, sea, and air assets, including legacy systems; (2) apply advanced technological solutions to increase performances of surveillance functions; (3) develop and demonstrate significant improvements in detection, tracking, identification, and automated behaviour analysis of all vessels, including hard-to-detect vessels, in open waters as well as close to coast.	June 2010	45 months	€15.6m (€9.9m)	SELEX (Finmeccanica)
OPARUS (Open Architecture for UAV-based Surveillance System)[236]	(1) The integration of UAVs/drones into EUROSUR by defining the "open architecture for the operation of unmanned air-to-ground wide area land and sea border surveillance platforms in Europe", taking into account the draft legislation for insertion of UAVs into civilian airspace currently being drafted by the European Commission and EUROCONTROL (the pan European Civil	Sept. 2010	18 months	€14m (€11.9m)	Sagem

234 PERSEUS, available at: http://www.perseus-fp7.eu/.
235 SEABILLA, available at: http://www.seabilla.eu/cms/.
236 OPARUS, available at: http://www.oparus.eu/.

	Aerospace Association); (2) demonstrate drone surveillance, secure datalinks, communication networks, and a generic ground control station.				
I2C (Integrated System for Interoperable sensors and Information sources for Common abnormal vessel behaviour detection and Collaborative identification of threat)[237]	To combine radar and vessel-tracking systems together with new prototypes and sensor technologies to create an "all weather traffic surveillance" system that it claims will be able to "track small crafts" over a "wide maritime zone [of] up to 200 nautical miles". Will incorporate data from "deployable sensor platforms" including aircraft and vessel patrols, unmanned submarine vehicles (USVs), and "Zeppelin" airships, which offer "absolute quiet flight with no vibration for high resolution observation quality and a payload of 2 tons for sensors and communication devices." Promises EUROSUR a "common intelligent operational traffic picture appending to vessel tracks information [sic] on performed activities, flags, sea state conditions, regulations, etc"; the capacity to "detect abnormal vessel behaviours and issue automatically alarms to operator for validation".	Oct. 2010	4 years	€16m (€9.9m)	DCNS (French naval contractor)
EFFISEC (EFFicient Integrated SECurity Checkpoints)[238]	(1) To enhance the security and efficiency of land and maritime checkpoints through technology; (2) improve the working conditions for border inspectors; (3) increase flow of people crossing borders.	May 2009	4 years	€16.3m (€10m)	Sagem
WIMAAS (Wide maritime area airborne surveillance)[239]	Provide the airborne building block of maritime surveillance with the potential for reduced cost of operation, more autonomous and improved efficiency through the introduction of air vehicles with reduced or zero onboard crew [drones] (…) You cannot control what you do not patrol. Even if cooperation is crucial, air assets are a unique capability for wide-area maritime surveillance because they provide situation awareness over extended areas (endurance, speed, and long-distance detection), re-direction to areas of interest (threat) and flexible reaction (inspection when needed). WiMA²S will	Dec. 2008	3 years	€40m (€27.4m)	Thales

237 I2C project, # 242340.
238 EFFISEC, available at: http://www.effisec.eu/.
239 ARGUS 3D, available at: http://www.argus3d.eu/project.

	develop concepts and technologies for better operational use at lower costs of Maritime Surveillance Manned Airborne Vehicle, and Maritime Surveillance Optionally Piloted Vehicles because regulations will not allow UAVs to fly across European Airspace for years to come.				
ARGUS 3D (AiR Guidance and Surveillance 3D)[240]	To improve the detection of manned and unmanned platforms by exploiting the treatment of more accurate information of cooperative as well as non-cooperative flying objects, in order to identify potentially [sic] threats (…) The final objective of the research consists of study, design and realisation of a simple demonstrator of a low-cost, interoperable, radar-based, system	Dec. 2009	3 years	€49.4m (€32.6m)	SELEX (Finmeccanica)
AMASS (Autonomous maritime surveillance system)[241]	To facilitate observation and security of wide critical maritime areas in order to reduce actual and potential illegal immigration and the trafficking of drugs, weapons, and illicit substances. The surveillance system will consist of autonomous, unmanned surveillance buoys with active and passive sensors, the key sensors being un-cooled thermal imagers connected as a network with wideband radio.	Mar. 2008	42 months	€5.5m (€3.6m)	Carl Zeiss Optronics
SECTRONIC (Security system for maritime infrastructure, ports and coastal zones)[242]	To develop "a 24h small area surveillance system that is designed to be used on any ship, platform, container/oil/gas terminal or harbour" using "all accessible means of observation (offshore, onshore, air, space) (…) exchanged via an onshore control center."	Feb. 2008	4 years	€4.1m (€2.8m)	Marine & Remote Sensing Solutions Ltd
UNCOSS (Underwater Coastal Sea Surveyor)[243]	To develop tools for the non-destructive inspection of underwater objects mainly based on neutron sensors.	Dec. 2008	4 years	€4.1m (€2.8m)	French Atomic Energy Agency
TALOS (Transportable autonomous patrol for land	To field-test "a mobile, modular, scalable, autonomous and adaptive system for protecting European borders" that will "take measures to stop the illegal action	June 2008	4 years	€19.9m (€12.9m)	PIAP (Polish defence contractor)

240 ARGUS 3D, available at: http://www.argus3d.eu/project.
241 AMASS project, http://www.amass-project.eu/amassproject/.
242 SECTRONIC, available at: http://www.sectronic.eu/.
243 UNCOSS, available at: http://www.uncoss-project.org/.

border surveillance)[244]	almost autonomously with supervision of border guard officers." Uses drones and unmanned land vehicles.				
CONTAIN (Container Security Advanced Information Networking)	To support transport security stakeholders in managing container security threats as part of an integrated approach to the management of transportation networks; provide a coherent set of technology options for screening and scanning, plus container-integrated sensor, communication, and security technologies to monitor container movements and security-related parameters in real time; enable ports to establish upgraded port container security processes; and provide information feeds to port community systems and national and European security databases.	Oct. 2010	42 months	€15.6m (€10m)	TNO (Swedish Defence Research Institute)
GLOBE (European Global Border Environment) [245]	To provide a comprehensive framework in which an integrated global border management system must be developed (…) moving throughout the four main layers of border control (country of origin, transit areas, regulated and unregulated border lines, and internal territory). Described as the "first phase" in the EUROSUR demonstration project.	July 2008	12 months	€15.6m (€10m)	Telvent (Spanish IT company)
OPERAMAR (interoperable approach to the European union maritime security management) [246]	To provide the foundations for pan-European Maritime Security Awareness by addressing the insufficient interoperability of European and national assets with a view to generating unified data models for seamless exchange and contributing to address the discrepancies of the behavioural, organisational, and cultural issues.	Mar. 2008	15 months	€0.7m (€0.7m)	Thales
STABORSEC (Standards for border security enhancement) [247]	To produce an inventory of needed standards for stand-alone equipment used for border security.	Feb. 2007	18 months	€0.7m (€0.5m)	Sagem
SOBCAH	To identify the main threats relevant to	Feb.	18	€3m	Galileo Avionica

244 TALOS, available at: http://talos-border.eu/.
245 GLOBE project, # 218207.
246 OPERAMAR final report, available at: http://cordis.europa.eu/search/index.cfm?fuseaction=result.document&RS_LANG=EN&RS_RCN=11485692&q=.
247 STABORSEC flyer, available at: ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/straborsec_en.pdf.

(Surveillance of Borders, Coastlines and Harbours)[248]	"green" and "blue" borders; elaborate the most suitable architectural solutions based on the most advanced existing sensors and network technologies; execute a proper modelling of the established solution; carry out the technology validation of the selected solution, first in the laboratory and then in the port of Genoa (Italy); elaborate a consistent road map.	2006	months	(€2m)	(Finmeccanica)

4.2.2 Space-based border surveillance and the Common Information Sharing Environment

Global Monitoring for Environment and Security is the EU's programme for the establishment of a European capacity for Earth observation. GMES is also funded from the FP7 budget, accounting for approximately 85 per cent of the €1.4 billion space programme in FP7, which runs from 2007–2013. When it was launched, GMES – then Global Monitoring for *Environmental* Security – was focussed solely on environmental information, with no envisaged security or defence capacities, but like the ESRP, it has increasingly been used to support the development and implementation of EUROSUR and the Common Information Sharing Environment. As well as using GMES services, the Common Application of Surveillance tools provided for in the draft Regulation will see FRONTEX purchase satellite imagery from private providers through the EU Satellite Centre.

Box 5 details seven GMES projects that have directly or indirectly supported the development of EUROSUR or the broader Common Information Sharing Environment. Total EU funding for these projects is more than €36 million to date, yet a total budget of just over €60 million was provided for in the EUROSUR Financial Study for the period 2011–2020. The total R&D investment for EUROSUR has clearly been underestimated in the EUROSUR Financial Study and Commission Impact Assessment. In addition to FP7-funded R&D, the European Commission has also funded two pilot projects to develop the Common Information Sharing Environment envisaged by its integrated maritime surveillance policy. These are MARSUNO (focussing on the North Atlantic)[249] and BLUEMASSMED (focussing on the Mediterranean),[250] which had a combined budget of more than €5 million.

248 SOCBAH flyer, available at: ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/sobcah_en.pdf.
249 MARSUNO, available at: http://www.marsuno.eu/project/.
250 BLUEMASSMED, available at: http://www.bluemassmed.net/.

Box 5: GMES projects supporting EUROSUR

Name	Objective	Start date	Dur-ation	Cost (EU contrib -ution)	Led by
MARISS (MARitime Security Service)	The integration of coastal radar information, Vessel Detection Systems, Vessel Traffic Management Systems, and Automatic Identification Systems, with airborne and Earth Observation data.	Nov. 2005	10 months	n/a	Telespazio (Finmeccanica)
TANGO (Telecomm-unications advanced networks for GMES operations)[251]	To develop, integrate, demonstrate, and promote new satellite telecom services dedicated to GMES. TANGO is the first project under EC FP6 focussing on the use of satellite telecom to serve the needs of the whole GMES community. The project addresses key environment and security applications.	Nov. 2006	36 months	€9.3m (€5.2m)	EADS Astrium
LIMES (Land and sea integrated monitoring for European security)[252]	To define and develop prototype information services, based on satellite technology, to support security management at EU and global level [for]: organisation and distribution of humanitarian aid and reconstruction; surveillance of the EU borders (land and sea); surveillance and protection of maritime transport for sensitive cargo; protection against emerging security threats (e.g. terrorism, illegal trafficking, proliferation of weapons of mass destruction).	Dec. 2006	42 months	€21.2m (€11.9m)	Telespazio (Finmeccanica)
GMOSAIC (GMES services for management of operations, situation awareness and intelligence for	To identify and develop products, methodologies, and pilot services for the provision of geo-spatial information in support of EU external relations policies and demonstrate the sustainability of GMES global security perspective.	Jan. 2009	39 months	€15.2m (€9.6m)	E-GEOS Spa (Telespazio-Finmeccanica)

251 TANGO, available at: http://www.teladnetgo.eu/.
252 LIMES flyer, available at: http://www.fp6-limes.eu/uploads/docs/LIMES-PRS.004-TPZ%20%5BInfosheet%5D.pdf.

regional crises)[253]					
NEREIDS (New Service Capabilities for Integrated and Advanced Maritime Surveillance)[254]	Enhanced EO capabilities by combining different sensors with innovative data-fusion techniques; a toolbox approach enabling the sharing of data and supporting the common maritime picture.	June 2011	36 months	€6m (€4m)	GMV Defence & Security
SIMTISYS (Simulator for Moving Target Indicator System)[255]	Maritime surveillance for safety purposes as border surveillance, traffic safety, fishery control, and environmental protection and monitoring; the tracking of small vessels.	June 2011	30 months	€2.5m (€1.6m)	Thales Alenia
DOLPHIN (Development of Pre-operational Services for Highly Innovative Maritime Surveillance Capabilities)[256]	To develop the key technological and operational gap-filling innovations, leading in the mid-term to a full and sustainable operational exploitation of Earth Observation Satellite capabilities in the EU and MS maritime policies applications. DOLPHIN aims at developing new tools providing effective improvements of state-of-the-art capabilities in maritime surveillance.	June 2011	30 months	€7.1m (€4m)	E-GEOS Spa (Telespazio-Finmeccanica)

4.2.3 EU funded R&D projects supporting smart borders

Whereas the EUROSUR system has supported the range of projects detailed above, the EU is only just beginning to fund R&D for smart borders. The Total Airport Security System, for example, is a four-year, €15 million project that was launched in April 2010 and is being led by Israel's Verint Systems; the EU has contributed €9 million to the project thus far. The 2011 FP7-Security Call for Proposals called directly for projects supporting a Registered Traveller Programme and Automated Border Control. One or two large-scale demonstration projects are expected to be funded. It is regrettable that the European Commission did not wait until the member states had agreed on the general approach and the question of whether even to establish an EU RTP before committing substantial EU funds towards R&D in support of that objective.

253 GMOSIAC, available at: http://www.gmes-gmosaic.eu/.
254 NEREIDS, available at: http://www.nereids-fp7.eu/.
255 SIMTISYS flyer, available at: http://ec.europa.eu/enterprise/policies/space/files/simitisys_en.pdf.
256 DOLPHIN, available at: http://www.gmes-dolphin.eu/.

4.3 Funding the implementation of EUROSUR and smart borders

In addition to using the EU's research programme to fund its R&D into smart borders and EUROSUR, the European Commission has used two generic funding programmes – the External Borders Fund and the migration cooperation programme of the Development Cooperation Instrument – to fund the implementation of the EUROSUR system in the member states and third countries. From 2013, these programme instruments will be merged into the proposed €4.7 billion Internal Security Fund 2014–2020.

4.3.1 The EU External Borders Fund

Money from the External Borders Fund (EBF) has been available to the member states to establish or modify their National Coordination Centres in order to participate in EUROSUR for the past four years. In August 2007, the European Commission adopted strategic guidelines on the implementation of the €1.8 billion External Borders Fund (EBF, 2007–2013) prioritising "support for the development (…) of the national components of a European Surveillance System."[257] The European Parliament was not consulted (the EUROSUR roadmap would not be proposed for another six months).

Almost half of the total EBF for 2007–2013, some €800 million, is allocated to three priority areas: the "improvement of [national] border surveillance capacities in terms of infrastructure and equipment"; establishing/modifying National Coordination Centres; and "interlinking and integrating the existing communication systems into one comprehensive surveillance system."[258]

Insufficient information regarding the use of the EBF is available to assess how much has been spent on EUROSUR to date, though the EUROSUR Financial Study estimated the costs of "setting-up, upgrading and maintaining" the National Coordination Centres at €194 million for the period 2011–2016 (see Figure 8). The European Commission's 2011 impact assessment, however, provided an estimate of only €99.6 million for the NCCs for the period 2011–2020, with the same amount envisaged for the FRONTEX Situation Centre. The draft EUROSUR Regulation, meanwhile, envisages spending €112 million from the Internal Security Fund 2014–2020 on the NSCs and a further €132 million over the same period for the FRONTEX Situation Centre and Common Pre-frontier Intelligence Picture (approximately two-thirds of which will come from the ISF).[259]

257 Decision 2007/599/EC (EBF strategic guidelines, priority 2); see further Decision 2008/456/EC on implementing rules for EBF and Decision 2010/69/EU amending the 2008 rules to allow funding of national infrastructure.
258 COM (2011) 857 final, p. 10.
259 COM (2011) 873 final, p. 35.

Figure 8: Cost of establishing, upgrading, and maintaining NCCs 2011–2026[260]

Country	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	€ -	€ -	€ -	€ -	€ -	€ -	€ -
Total	**€ 28,383,951**	**€ 42,524,795**	**€ 34,772,400**	**€ 31,131,036**	**€ 28,280,942**	**€ 28,821,448**	**€ 193,914,573**

4.3.2 The Development Cooperation Instrument

A key object of EUROSUR is to integrate existing regional surveillance systems for border control/internal security purposes into the EUROSUR network. In particular, FRONTEX wishes to integrate operational data from the SEAHORSE ATLANTIC,[261] Baltic Sea Regional Border Control,[262] and Black Sea Border Coordination[263] networks into EUROSUR. Between 2007 and 2010 the cost of upgrading and maintaining the technical infrastructure of these and a third regional cooperation centre covering the Baltic States was €77 million.[264]

For the period 2011–2013, the European Commission has allocated "between 15 and 25 per cent" of the €179 million "Thematic programme for cooperation with third countries in the areas of migration and asylum", part of the EUROPAID Development Cooperation Instrument, to "third countries situated along the southern and south-eastern maritime borders… which accept to

260 Source: SEC (2011) 1538 final, p. 35.
261 SEAHORSE ATLANTIC is a network between border control authorities in Spain, Portugal, Mauritania, Morocco, Senegal, Gambia, Guinea Bissau, and Cape Verde for exchanging information on "irregular migration and criminal activities" along the coastlines of North and West Africa and the Canary Islands.
262 Baltic Sea Region Border Control Cooperation is a network of Coordination Centres between Estonia, Denmark, Finland, Germany, Latvia, Lithuania, Poland, Sweden, Norway, and Russia.
263 The Black Sea Border Information Center, located in Bourgas, Bulgaria, is an initiative of the Black Sea Cooperation Forum comprising border guards from Bulgaria, Romania, Ukraine, Russia, Georgia, and Turkey.
264 Source: SEC (2011) 1538 final, p. 55.

cooperate in the framework of EUROSUR."[265] This is substantially more than the €5 million the Commission estimates it will cost to incorporate third countries and regional networks. In 2011 the Spanish interior ministry submitted a proposal to establish SEAHORSE MEDITERRANEAN, modelled on SEAHORSE ATLANTIC, using funds from the EUROPAID thematic programme.[266] In addition to concerns about the exchange of data with third countries that do not have equivalent human rights standards, the use of the EU development budget to fund the implementation of EU security policies is lamentable. As others have pointed out, it may also contribute to a restriction of the rights of people to leave a country to seek asylum.[267]

4.3.3 The Internal Security Fund

The European Commission has proposed the allocation of €3.5 billion from the €4.7 billion Internal Security Fund 2014–2020 to external borders and visas, including large-scale IT systems.[268] The priorities for the fund are "[T]he further development of an integrated border management system by improving, replacing, and upgrading equipment/infrastructure for visa and borders according to new technological developments. This would in particular include enhancing the operational capabilities of the member states within the framework of EUROSUR standards." As noted above, the Commission has indicated that €200 million could be made available to support the development of the NCCs and FSC.

The ISF will also support

> "enhance[d] cooperation with third countries and to reinforce certain key aspects of their border surveillance and management capabilities in areas which are of particular interest and which have a direct impact in the EU. For example, in the framework of EUROSUR, funding could be made available to link third countries' systems and infrastructures to the EU's in order to allow for the regular exchange of information."[269]

"Without prejudice to the future proposals from the Commission on the smart borders package and the subsequent decision of the European Parliament and the Council," the European Commission has also allocated almost one-third of the ISF to implementing those proposals.[270] "The cost of developing a central and national systems for EES and RTP has been estimated between about 1 and 1.3 billion EUR (...) On the basis of these assumptions and given that development would only start as from 2015, it is proposed to set aside 1.1 billion EUR for these two systems under this proposal."[271] It is regrettable that the implementation of the EUROSUR and smart borders proposals is effectively outsourced to a generic funding instrument. At least in the case of the proposed EES and RTP, the newly established EU Agency for Large-scale IT Systems would be responsible for the new projects. Where EUROSUR is concerned, the Agency has been expressly excluded from any role

265 Commission Decision OJ C 2011/2304, 7 Apr. 2011; see also SEC (2011) 1536 final, p. 17.
266 SEAHORSE presentation, available at: http://www.imp-med.eu/En/En/image.php?id=125.
267 "Analysis of the external dimension of the EU's asylum and immigration policies – Summary and recommendations for the European Parliament", Brussels: European Parliament DG for External Policies of the EU, PE 374.366 (2006), pp. 10–11.
268 COM(2011) 750 final, 15 Nov. 2011.
269 COM (2011) 749 final, 15 Nov. 2011, p. 8.
270 COM (2011) 750 final, p. 6.
271 Idem, p. 8.

on the grounds of political expediency. It is questionable to say the least whether FRONTEX and the European Commission have the experience or expertise to implement such an ambitious proposal.

Figure 9: Questioning the EUROSUR cost estimates

Cost	Commission estimate	Our estimate	Based on
National Coordination Centres	€99.6 million	€227 million	MS estimates of €105 million for 2011–2013 (see Figure 8) plus €112 million indicative ISF 2014–2020 allocation in draft EUROSUR Reg.
FRONTEX Situational Picture & Common Pre-Frontier Intelligence Picture	€129.2 million	€152 million	FRONTEX estimate of €20 million for 2011–2013 (in Commission impact assessments), plus €132 million indicative ISF 2014–2020 allocation in draft EUROSUR Reg.
Communication network	€46.7 million	€46.7 million	
Common application of surveillance tools	€29.6 million	€350 million	Approximately €35 million per annum spent on EUROSUR related R&D projects in 2010–2012, extrapolated over 10 years. Note that EUROSUR is included as an explicit R&D priority in Horizon 2020 and a substantial increase has been proposed for the overall security budget.
Networks with third countries	€5.4 million	€98 million	Approximately €38 million allocated from DCI Thematic programme on migration 2011–2013, extrapolated over 10 years. Costs of incorporating third countries into EUROSUR to come from ISF from 2014.
Total	**€338.7 million**	**€873.7 million**	

4.4 The United States' experience: SBI-net and US VISIT

It is also regrettable that the European Commission has not apparently considered the perceived successes and failures with regard to comparable large-scale border control initiatives in the United States in its impact assessments of EUROSUR, the Entry-Exit System or Registered Traveller

Programme. The proposed EES is not unlike the US VISIT programme, which collects biometric data from all entrants. US VISIT was established in 2004 and began collecting two fingerprints from persons subject to the USA's visa requirements. By 2009 the programme was collecting all ten fingerprints and had been extended to nationals of states not subject to the visa requirement, including EU citizens. As Peers notes,

> the Commission's 2008 impact assessment does not indicate how many persons are likely to be detected on the territory or refused entry at the border or refused visas as a result of an entry-exit system. Such estimates are crucial to assessing the added value of such a scheme. As the EDPS has pointed out, the US system has led to 1300 refusals at the border, at the cost of $1.5 billion. This amounts to a cost of over $1 million per refused entrant – although it is possible that the US system has had other results as regards the objectives of immigration control.[272]

In addition to the substantial costs, the USA has been unable to complete the US VISIT programme, which initially envisaged recording the exit of all foreign nationals as well as their entry. In 2009, the US Government Accountability Office (GAO) found that the Department of Homeland Security "lacked a detailed schedule for implementing an exit capability, and that, among other things, cost estimates for the then proposed exit solution were not reliable, risk management was not being effectively performed, and the program's task orders were frequently rebaselined". Two-and-a-half years later, there has been no apparent progress toward a functional exit component for US VISIT.

Any reflection on the United States' experience with its $3.7 billion Secure Border Initiative (SBI-net) would have been equally sobering. Launched in 2006, SBI-net was supposed to establish a "virtual fence" using a complex network of high-tech surveillance equipment to police the entire northern border (with Canada) and southern border (with Mexico), but in 2010 funding was frozen. Testifying before Congress, US Homeland Security Secretary Janet Napolitano described the project as "plagued with troubles from day one (…) It has never met a deadline, it hasn't met its operational capacities, and it doesn't give us what we need to have."[273] In 2008, the GAO had highlighted the nature of the problems with SBInet:

> Important aspects of SBInet remain ambiguous and in a continued state of flux, making it unclear and uncertain what technology capabilities will be delivered, when and where they will be delivered, and how they will be delivered. For example, the scope and timing of planned SBInet deployments and capabilities have continued to change since the program began and, even now, are unclear. Further, the program office does not have an approved integrated master schedule to guide the execution of the program, and GAO's assimilation of available information indicates that the schedule has continued to change. This schedule-related risk is exacerbated by the continuous change in and the absence of a clear definition of the approach that is being used to define, develop, acquire, test, and deploy SBInet.[274]

While elements of the SBInet programme remain, it is important to recognise that whereas the framework for federal government accountability in the United States allows for critical audits of projects like SBI-net and US VISIT by impartial technology experts, there is no comparable body to oversee EU security technology projects. The GAO in particular produces detailed reports that

272 Peers "Proposed new border control systems", p. 9.
273 *Defence Industry Daily*, 16 Jan. 2011.
275 GAO, "Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment", September 2008, p. 2.

properly assess the achievements and failures of large-scale IT projects as against their cost and stated objectives.[275] Should the EU decide to press ahead with its own smart borders initiatives, it is imperative that more stringent mechanisms for democratic oversight and control are introduced, particularly with regard to EUROSUR.

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

5 Conclusions

More than four years have now passed since the European Commission published its 2008 smart borders package. The European Parliament and the Council have started negotiating on the legislative proposal for EUROSUR; within months the Commission is expected to publish legislative proposals on the Entry-Exit System and the Registered Travellers Programme. Since only limited discussions that have taken place within the European Parliament and among the member states in the EU Council, we are concerned that the likely cost, fundamental rights impact, and potential effectiveness of the three systems has not been properly debated or thought through. The various impact assessments produced by the Commission have failed to demonstrate the necessity of the planned systems in terms of effectively controlling immigration, significantly enhancing the security of EU citizens, or facilitating travels of third-country nationals. In the absence of such justifications, the proportionality of EUROSUR, EES, and RTP is strongly open to question.

In many respects, it is the wider EU policy context that is responsible for the most acute concerns about the three proposed systems. The EU's "Global Approach on Migration and Mobility" seeks explicitly to externalise EU migration controls by creating immigration "buffer zones" outside of EU territory and cooperating with third countries to prevent the departure of migrants and refugees bound for Europe. Human rights organisations have challenged the legitimacy of this policy, arguing that it encourages "push back operations" that result in the circumvention of the EU's obligations under the Geneva Conventions and breaches of the *non-refoulement* principle that prohibits the transfer of persons to territories where that person faces the risk of torture or inhuman and degrading treatment. EUROSUR's draft legislation is ominously silent on this point, though the European Commission and FRONTEX argue that EUROSUR has the express aim of saving lives at sea – an objective that finds strong support in international law. In practice it will be the way in which FRONTEX and the member states actually prioritise search-and-rescue and asylum protection over surveillance, interception and so-called push back operations that will determine the legitimacy of EUROSUR in the eyes of many observers. While certain safeguards may be added to the draft Regulation, these issues are likely to remain largely beyond the scope of the draft legislation. It is, however, imperative that the tacit extension of FRONTEX's remit and powers envisaged by the EUROSUR legislation is accompanied by greater democratic control and measures to ensure compliance with international law, including stricter rules governing cooperation with third states and agencies, clearer procedures for joint operations and clarification of the EU's *non-refoulement* obligations.

The EES and RTP proposals must also be seen in a broader policy context. The European Union has already established three vast immigration databases: the Schengen Information System (SIS), to detect and exclude "illegal" aliens and persons posing a threat to the security of the member states; EURODAC, which houses the fingerprints of all asylum applicants; and the Visa Information System (VIS), which is accompanied by some of the most stringent visa requirements in the world. The introduction of "biometrics" (fingerprint data) into the second generation of SIS and the VIS, which share a biometric matching system, will create one of the world's largest fingerprint databases. The proposed EES would supplement these existing systems by recording the identity and movements of

tens of millions of third-country nationals not currently subject to a visa requirement, and automatically flagging potential overstayers. Just as EUROSUR is emblematic of a paradigm shift in the policing of the open seas, the EES and RTP proposals symbolise the "next step" in the roll-out of EU-wide biometric immigration systems. The proposals certainly appear to us as much a product of this political and economic momentum than a rational, cost-effective response to a perceived migration crisis. The Registered Travellers Programme is conceived as a way of offsetting the inconvenience of more stringent checks, but in practice it is only likely to be available to a small category of pre-vetted business travellers.

The proposals must also be considered in light of the ongoing financial crisis and the impact of austerity measures. The European Commission has estimated that the three systems could cost at least €1.5 billion. This is a massive investment in large-scale IT systems, the need for which – and potential effectiveness of – remains in serious doubt.

5.1 EUROSUR

The proposed European Border Surveillance System is an ambitious and costly project with important implications for fundamental rights and the development of EU policy towards migrants and refugees more generally. It is troubling that whereas comparable systems such as the Schengen and EUROPOL Information Systems have been developed on the basis of "primary" (enabling) and "secondary" (implementing) legislation – which was to a limited extent at least discussed in the European and national parliaments, and by civil society – in the case of EUROSUR, this method has been substituted with a technocratic process that has allowed for the development of the system and substantial public expenditure to occur well in advance of the legislation now on the table.

Implementing the 2008 EUROSUR roadmap – before any proper debate or formal consultation procedure could take place – has left little room for discussion of the necessity and proportionality of the proposed system in light of the expected costs and potential fundamental rights implications. Following five years of development, the European Commission expects to adopt the legal framework and have the EUROSUR system up and running (albeit in beta form) in the same year (2013), presenting the European Parliament with an effective fait accompli. While the Parliament is simply expected to fine-tune the proposal, it does have the opportunity to introduce some crucial safeguards. The Parliament should also ensure that the legal and financial frameworks for future initiatives, such as the Common Information Sharing Environment for EU maritime surveillance, EES, and RTP, are adopted before the development of the proposed systems commences.

As noted above, the justification for EUROSUR rests on its potential to combat "illegal immigration", increase European security, and save lives at sea. These claims must be treated with caution. On the one hand, they rely on the as yet unproven interoperability of new technologies; on the other, the EUROSUR proposal fails to guarantee the primacy of search and rescue functions. Assuming the technology works, EUROSUR could clearly help to bring more people to "safety". There is, in fact, a compelling case for a significant investment of financial and human resources in saving lives in the Mediterranean, but nowhere in the proposed EUROSUR Regulation and numerous assessments, studies, and R&D projects, is it defined how exactly this will be done, nor are there any procedures laid out for what to do with the "rescued". The boats that FRONTEX hopes to detect using EUROSUR typically contain irregular migrants and persons in need of international protection, but nothing is

said about the requirement to process requests for asylum. If FRONTEX and the European Commission are serious about EUROSUR's proclaimed aim to save lives at sea, the draft Regulation must be amended so that search and rescue obligations are prioritised and read jointly with the requirements of refugee law and human rights law. At a minimum the proposal must specify how EUROSUR will send information or alerts to the Rescue Coordination Centres of the country responsible for a specific Search and Rescue Region. It must also be made clear to FRONTEX and the member states that they cannot equate interception measures on the high seas to prevent migrants from reaching Europe's borders with search and rescue missions. The latter must be prioritised and include the positive obligations stemming from the UN Convention on the Safety of Lives at Sea and refugee laws spelt out by the European Coastal Patrols Network, regional cooperation networks such as SEAHORSE, and any third states invited to participate in EUROSUR.

We are equally concerned about the technical viability of the proposal. Despite the high-tech claims about "continuous 24/7 surveillance", "situational pictures", and "pre-frontier intelligence", the planned EUROSUR system has not been subject to a proper technological risk assessment. EUROSUR relies on the implementation of a host of new technologies and the interlinking of 24 different national coordination centres and surveillance systems – bilaterally and through FRONTEX. This process will be both extremely complex and extremely costly, yet the only people who have been asked if they think it will work are FRONTEX and the companies selling the technology. We see no logical or justifiable reason for rushing the process of establishing EUROSUR or excluding bodies like the new EU Agency for Large-scale IT Systems. On the contrary, the results of the numerous R&D projects funded by the European Commission now enable a fuller evaluation of the proposed EUROSUR system and the prospects for success of a whole range of detection and communications technologies to take place before further EU funds are committed.

As currently developed, the legislative and financial framework for EUROSUR appears to give a blank cheque to FRONTEX and the European Commission to keep funding R&D from the EU budget until they find something that works. EUROSUR itself has not been properly costed and, as shown in Figure 9, above, the estimates provided by the European Commission do not stand up to even the minimal scrutiny provided in this report. Funding EUROSUR from different multi-annual budget lines – over which the European Commission and FRONTEX enjoy a large degree of discretion in regard to the annual funding priorities – appears a recipe for financial excess. Based on recent expenditure and indicative budgets for the Internal Security Fund, it appears that EUROSUR could easily end up costing two or three times the Commission's estimate (see Figure 9, above). Without a cap on what can be spent attached to the draft EUROSUR, Horizon 2020, and Internal Security Fund legislation, the Parliament will be powerless to prevent any such cost overruns. The Parliament should also seek clarification over the extent to which the draft EUROSUR legislation envisages the purchase of "drones" and other common surveillance tools by FRONTEX from EU funds, and ensure that this is subject to democratic debate and appropriate controls with regard to public safety and civil liability.

It is also highly problematic that there is no single mechanism for financial accountability beyond the periodic reports submitted by FRONTEX and the European Commission from October 2015. In the continued absence of concise reports about EUROSUR-related expenditure within FRONTEX and across the various EU budget lines, it is already extremely difficult to monitor what has actually been spent on the project. By excluding the EU Agency for Large-scale IT Systems, the broader prospects for accountability around EUROSUR's development are also greatly diminished. Finally, given that

EUROSUR seeks primarily to address "illegal migration" at sea, we see no need to introduce the landlocked or northern European member states into EUROSUR from the outset. Given the financial constraints of the current climate, it is surely advisable to develop EUROSUR more slowly – initially as a communications network for the 10 member states that are part of the existing European Coastal Patrols Network, with new technologies and member states integrated into the network as, and when, (i) a clear need arises and (ii) their inclusion can be justified.

The EUROSUR Regulation lacks adequate data protection safeguards. While EUROSUR will not gather a massive amount of personal or biometric data, or result in the establishment of a centralised database that stores such information, personal data could be processed in a number of different "layers" of the situational pictures. FRONTEX can use information from new surveillance systems, including drones, within the "common applications of surveillance tools" in order to supply the national coordination centres and itself with information on the external borders and on the pre-frontier area. EUROSUR will also perform the "border control" function of the EU's wider Common Information Sharing Environment, under which its information will be shared with a whole range of third actors, including defence agencies. All these capabilities raise a whole range of potential privacy and data protection concerns that are not adequately addressed in the current draft Regulation.

A specific provision that explicitly and exhaustively enumerates the conditions under which personal data may be processed in EUROSUR and exchanged with external bodies and agencies must be included in the legislation. Since the exchange of EUROSUR information with "neighbouring third countries" would take place on the basis of bilateral or multilateral agreements between the member state(s) and third countries, it is also crucial to mandate the logging of all such information exchanges in order to enable national supervisory authorities to properly review the sending of information to third countries and ensure that it does not lead to breaches of fundamental rights. The EUROSUR Regulation should also explicitly include a system of layered supervision – with national data protection authorities checking processing of personal data by the National Coordination Centres, and the processing of personal data by FRONTEX, subject to review by the European Data Protection Supervisor. It is currently unclear whether this form of layered supervision is envisaged by the draft Regulation.

Finally, we suggest that there must be greater democratic control of the implementation of the European Security Research Programme to mitigate against the corporate capture of the research agenda and the influence of defence and security contactors over the annual calls for proposals. This would ensure that EU-funded research complies with fundamental rights obligations from the outset while meeting a genuine need and providing value for money.

5.2 Smart borders

Both the EES and RTP envisage the creation of a centralised European database that will include potentially highly sensitive biometric data such as fingerprints and facial images from millions of people. All third-country nationals who want to enter the Schengen area would have no choice but to allow for the processing of their personal data. This scale of data-gathering must clearly demonstrate compelling grounds for public safety or public order in order to be considered a

proportional policy response. At present, the case for the pressing social need for either EES or RTP has not been made.

The principle justification for the EES is that it would lead to a more credible EU immigration policy by facilitating the return of visa overstayers. There are, however, major shortcomings with regard to this claim. There are many legal reasons that can explain the overstay of a person and many exceptions in the Schengen Border Code with regard to the registration of entry and exit, so an EES alert alone cannot be considered as grounds for expulsion or deportation. An overstayers alert can only ever constitute a *presumption* of illegal residence, and stringent follow-up controls with regard to the treatment of people identified as such will be needed to ensure that the EU respects its human rights obligations. An administrative procedure must be completed in order to determine whether the person has the right to stay legally in EU territory, and this procedure must give the traveller the chance to explain the circumstances of any overstay. It is currently also lawfully impossible to include an EES alert into the SIS/SIS II system, which only provides for the inclusion of deportation orders issued by a court or other competent authority. Given that there can be no immediate consequences for overstayers following an EES "hit", the extent to which this will lead to more efficient return operations is strongly open to question. Any attempt to automatically link EES alerts to the SIS/SIS II would also likely result in the stopping of an unacceptable number of perfectly innocent travellers. It must also be recalled that border guards already check the passports of departing visa holders for overstays; semi-automating this process will not reduce their workload, it will merely assist them in conducting such checks.

The EES will also surely result in longer queues for third-country nationals wishing to enter the Schengen area. Whereas TCNs subject to a visa requirement are already required to provide biometric data on entry, those on the so-called white lists who do not require an advance visa are exempt from this requirement. Extrapolating from border-crossing statistics collected during a comprehensive monitoring exercise in 2009, this could result in the fingerprinting of an additional 57 million "white list" TCNs. The VIS impact assessment of 2004 stated that, on average, 15 seconds were added to entry procedures in the United States when biometrics were collected for the US VISIT programme. If the EU were able to achieve this target with regard to 57 million TCNs, it would add the equivalent of 27 years of queuing time per year at the EU borders. Adequate provisions would also have to be made for "false positives", failures to provide biometrics, and a range of other eventualities.

The Commission proposes to offset these additional constraints on cross-border travel by establishing a Registered Traveller Programme that would enable registered travellers to cross borders much faster than their unregistered counterparts. The Commission has estimated that 4–5 million travellers might use RTP every year, yet 100 million TCNs are estimated to enter the Schengen area every year. Shorter queues at RTP gates witnessed to date are clearly the result of relatively fewer people being a part of such programmes (which typically charge an annual fee of around €125). There must be significant doubts, therefore, as to the RTP's capacity to relieve the pressure on Schengen borders or facilitate travel for the vast majority.

According to the Commission, the development of the central EES and RTP could incur costs in the order of €450 million, with annual operating costs of €190 million per year for the first five years.

The Commission has already allocated €1.1 billion to the development and implementation of these systems from the proposed EU Internal Security Fund 2014–2020, but since it is quite unclear at this stage whether these estimates assume that all Schengen states have fully implemented the Visa Information System, the ultimate costs could end up being much higher. Given that the VIS is not yet fully functional and the European Commission and its technology partners have not yet been able to successfully implement SIS II, it seems preposterous that the EU could be about to embark on another large-scale IT project before the effectiveness of either of these two systems has even been properly evaluated. Instead of creating a costly centralised RTP programme, it would surely be better at this stage to focus on interoperability between those states that have already local or national programmes and then assess the need for an EU-wide system after that.

6 Recommendations

We have been asked to provide recommendations for safeguards that could be introduced into the draft EUROSUR Regulation and any future legislation establishing the EES and RTP. As noted above we harbour substantial concerns about the EUROSUR legislation as currently drafted, and are not convinced of the need for either EES or RTP. We also harbour strong reservations about the current trajectory of EU border control policy and the role that increased surveillance plays in this context. We therefore begin with some general recommendations about the EU migration policy framework before specifically addressing the protection of fundamental rights and increased democratic control with regard to the draft EUROSUR legislation and the expected EES and RTP proposals.

6.1 The broader EU migration policy framework

- The mass surveillance and the treatment of all travellers as potential suspects is not a legitimate, necessary, effective or desirable cornerstone for EU migration policy. The EU should reconsider these policy initatives in favour of policy instruments that limit surveillance to that which is absolutely necessary, preserve fundamental rights and address migration control through more appropriate and accessible policy instruments.

- The externalisation of European immigration controls and the use of aid and technical assistance channels to create 'buffer zones' in which migrants and refugees are policed and detained by third countries according to the security demands of the EU is incompatible with the EU's stated development and human rights policy objectives. The EU should reorient its approach to relations with third countries in the field of migration around a human security-centred agenda.

- The increasing role of the security and defence industries in developing and implementing EU border control policies (which concomitant with the exclusion of civil society and human rights groups) is prone to serious conflicts of interests. The EU should reassess its intense partnership with the security industry in the context of obligations stemming from the Treaties to ensure that such risks are minimised while a balanced representation of views contributes to the formulation of policy.

6.2 EUROSUR

- Amend the draft EUROSUR Regulation to spell out the obligations of users of EUROSUR with regard to search-and-rescue and refugee and human rights law. This should include a clear articulation of the obligations stemming from the SOLAS Convention and a clear distinction between 'search and rescue' and 'surveillance and interception' missions.

- Introduce a specific provision in the draft EUROSUR Regulation that explicitly and exhaustively enumerates the conditions under which personal data may be processed in

EUROSUR and the conditions under which data can be provided to third actors, including defence agencies.

- Amend the draft EUROSUR Regulation to introduce a requirement for NCCs and FRONTEX to keep a logbook which keeps track of all transactions with third countries in order to enable national and/or European supervisory authorities to review the sending of information to third countries. This should be sufficiently detailed to ensure compliance with the prohibition in the draft legislative proposal on the exchange of information with a third country that could use this information to identify persons or groups of persons who are under a serious risk of being subjected to torture, inhuman and degrading treatment or punishment or any other violation of fundamental rights.

- Amend the draft EUROSUR Regulation to specify that there will be a system of layered supervision where national data protection authorities check the processing of personal data by the EUROSUR National Coordination Centres and the European Data Protection Supervisor oversees the processing of personal data by FRONTEX.

- Extend the provisions in the draft EUROSUR Regulation on financial accountability to require FRONTEX and the European Commission to provide an annual report detailing all expenditure on EUROSUR-related developments from all EU budget lines, including the External Borders Fund, proposed Internal Security Fund, FP7 and Horizon 2020 and the Development Cooperation Instrument.

- The draft Horizon 2020 legislation should be amended to provide for European Parliamentary control over the annual Calls for Proposals. In the area of security and space research this process should ensure that calls for EU-funded research address fundamental rights concerns from the outset, meet a verifiable security need and provide value for money.

- Request the European Parliament's Science and Technology Options Assessment Panel to conduct a technological risk assessment, review the R&D funded by the EU, and conduct a privacy impact assessment of EUROSUR.

- The European Parliament should request the Fundamental Rights Agency to prepare an advisory report on how best to use the resources available to the EU to enhance the safety at sea of migrants and refugees while ensuring the protection of fundamental rights.

6.3 Entry-Exit System and registered Traveller Programme

- Any future EES legislation must start from the assumption that an 'overstay' alert constitutes a *presumption* of illegal residence only. Once an alert has been issued, a proper procedure must be completed in order to determine whether the person has the right to stay legally in EU territory.

- Any future EES must take into account all of the current exceptions in the Schengen Border Code (especially in Annex VI and VII) that exempt certain persons from entry or exit stamps upon entering or leaving the Schengen area.

- Any future EES should provide for situations where persons have not been registered on entry or exit due to circumstances beyond their control. Such a situation may not lead to the issuing of an 'overstayer' alert.

- Any future EES should provide for the entry of third country nationals who were not able to (physically) enrol in a programme that uses biometric data.

- Any future EES should must include stringent data protection safeguards including the right to information for both applicants to the RTP as well as all TCN's whose data is processed within the EES. Information must be provided about:
    - the identity of the data controller,
    - the purposes for which the data will be processed
    - the categories of recipients of the data
    - the data retention period
    - the existence of the right of access to data relating to them, including
        - the right to request that inaccurate data relating to them be corrected or that unlawfully processed data relating to them be deleted
        - the right to receive information on the procedures for exercising those rights and the contact details of the National Supervisory Authorities which need to be able to hear claims concerning the protection of personal data

- Any future RTP and EES must provide for the applicant to be informed about the existence of remedies in the event that an application for an RTP has been denied, or when s/he has been classified as an 'overstayer'. Both systems must include the possibility to appeal or request a review of such decisions before a competent judicial or administrative authority, or a competent body composed of members who are impartial, who enjoy safeguards of independence in the Member State issuing the 'overstayers alert', and who are competent to judge the proportionality and the lawfulness of the measure.

- The need for access for law enforcement authorities to the EES, if any, must be demonstrated on a case-by-case basis and show the impossibility, or great difficulty, to obtain the data by other, less intrusive means. To enable review of this principle, a log book must be used to log all uses of EES data by law enforcement authorities. The use that will be made of EES data must be defined explicitly and restrictively, and go beyond general statements such as "necessary for the performance of their task." In this context the exact relationship between the EES and VIS and SIS/SIS II needs to be specified in the legislative proposal.

- Data from a third country national who has entered and left the territory in accordance with the rules has to be deleted immediately after verifying the 'exit'.

Authors

Dr. Ben Hayes is the Project Director at the London-based civil liberties organisation Statewatch, where he has worked since 1996, specialising in EU justice and home affairs policy, policing, criminal law, international relations, and international security. He is also a Fellow of the Transnational Institute (TNI), based in Amsterdam.

Mathias Vermeulen is a Research Fellow at the European University Institute (EUI) in Florence, Italy, and a part-time researcher at the Research Group on Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel, Belgium.