4 “EUROSUR on the Screen”

> When I first saw the EUROSUR on the screen,
> I finally realized what it was all about.
> *BG Major Świąteka*[1]

Today, EUROSUR is perceived and identified through the cartographic image of the European situational picture (ESP). The ESP, which is generated by a geographic information system (GIS) and visualized as a map with border-related information, emblematically stands for the exchange of information between EU member states and the Frontex agency. This “EUROSUR on the screen” is the object that is shown when the EUROSUR project is presented in public. For instance, when Erik Berglund, then Director of Capacity Building at Frontex, spoke about EUROSUR during a workshop at the European Parliament in 2012, he provided a screenshot of the map, commenting that this was what EUROSUR looked like.[2]

---

1 Border Guard Major Aleksandra Świąteka (Director of the International Relations Office, Polish Border Guard, Warsaw): “The Commission’s proposal for EUROSUR,” presentation during the conference “Keeping the EU’s External Borders Secure. Frontex and the Use of New Technologies” at the Academy of European Law (ERA) in Trier on May 15 and 16, 2012 [hereafter cited as BG Major Świąteka: EUROSUR Presentation (May 16, 2012)]. The statement quoted is from a bilateral conversation following her presentation.

2 Erik Berglund (Head of Capacity Building at Frontex): “European Border Surveillance System (EUROSUR): Objectives and State of Play,” presentation during the workshop “An Emerging e-Fortress-Europe? Border Surveillance, Frontex and Migration Control” at the European Parliament in Brussels on June 26, 2012, at: http://www.gruene-europa.de/an-emerging-e-fortress-europe-7509.html (accessed June 26, 2012).

This statement particularly and only gains relevance when considering that, during the first four years of the development phase – and thus also during the first years of my research – there was neither a map nor an image connected to the EUROSUR system. It was a vision that was lacking visualization. "How will it look" was thus an incredibly pressing question, particularly since the different elements that were supposed to be integrated by EUROSUR are quite heterogeneous: the 2008 EUROSUR Roadmap[3] mentions different authorities and existing surveillance systems, a vast amount of discontinuously generated information, such as occurrence reports by member states, Frontex's risk analysis, police and intelligence information from Europol, geodetic and meteorological data, daily news, close to real-time surveillance data sent by surveillance gadgetry such as radar or satellite, as well as information from the "pre-frontier area" provided, for instance, by Immigration Liaison Officers (ILO). In being able to "show" EUROSUR, Berglund allegedly demonstrated what the system amounted to, and that it all fit into one picture.

"How will it look?" was, however, more than a question of curiosity, which I as a researcher shared. The availability of a desktop IT application was also a critical element in the development phase, as the quotation heading this section illustrates. "When I first saw the EUROSUR on the screen, I finally realized what it was all about," Border Guard Major Aleksandra Świąteka, Director of the International Cooperation Bureau of the Border Guard Headquarters in Warsaw, reported of the pilot phase. Ostensibly, the electronic map – the "EUROSUR on the screen" – is where 'things' come together. According to Świąteka, seeing the electronic map helps to understand and justify the practical efforts and institutional restructuring that the European Commission has required of member state authorities in the development phase of the EUROSUR since 2008. It is on the screen where efforts come together.

This chapter inspects the "EUROSUR on the screen" in order to explore the drawing together and the concentration of efforts that went into the EUROSUR. The site-inspection explores the communication format that is offered and required by the application's graphical user interface (GUI). I start by describing the graphical features of the GUI, such as menu items and design. I then trace their development by looking into controversies and variations that preceded the technical implementation onscreen. Finally, the digital 'objects' and their devel-

3 European Commission (2008): Examining the Creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final (February 13, 2008), [hereafter cited as EUROSUR Roadmap, COM(2008) 68 final].

opments are correlated to their textual fixation in the EUROSUR Regulation. The chapter thus looks into the question of how political compromises are translated and operationalized into IT classifications, which in turn amount to binding rules in a regulation. Furthermore, the particularities of the European situational picture (ESP) and the Common Pre-frontier Intelligence Picture (CPIP) which also (e)merge "on screen" are discussed. The chapter ends with a discussion on visualization as the most powerful form of meditation in the EUROSUR network. The ESP lends the supranational EU border the necessary image and the necessary appreciation, thereby accomplishing a level of integration and Europeanization that hitherto and otherwise would have been impossible.

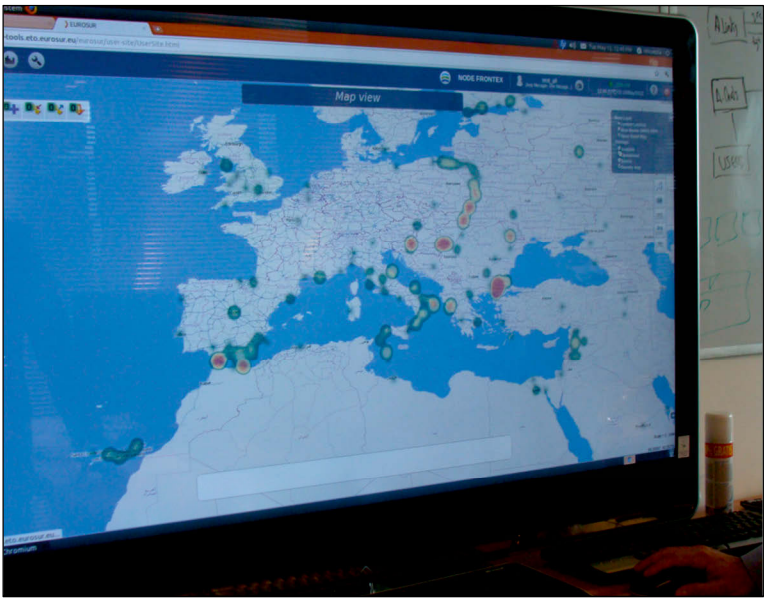
4.1 EUROSUR'S GRAPHICAL USER INTERFACE: COMMUNICATION DEVICE, FORMAT, NETWORK

Using the EUROSUR network means accessing a password-protected graphical user interface (GUI) on a personal computer. Once logged in, the user has access to an electronic map portraying the situation along the external borders of the EU in the form of a geo-tagged depiction of "border-related" information. The center of the GUI consists of a representation of the European continent in white on a light blue background. This acts as a kind of pinboard to which border-related information on a given geographical location can be added in the form of tags that include various expandable data fields. The interface has interactive features that allow the user to both read and input information.

The electronic map of the EUROSUR network and its graphical user interface were presented to me in the context of a "briefing"[4] with the responsible project manager for the EUROSUR network at Frontex in May 2012. The project manager has been in charge of the development, modeling and programming of the EUROSUR network and its graphical user interface since November 2009,

4 The "briefing" was offered to me instead of a participant observation in the Frontex Situational Center (FSC) that I initially asked for. This seemingly insignificant change of terms underlines how Frontex maintains the prerogative of interpretation. Neither the agency nor its services remain passive while under observation; rather, it is the agency who informs those "outside the border guard community" by means of a briefing. My object of investigation thus turned itself into the subject of explanation.

Figure 4: EUROSUR on the screen



Source: own photograph, taken in May 2012

and he has been discussing and negotiating the system's features with the participating member states since March 2010. During our conversation[5] he appeared to highly identify with the computer-generated network, which culminated in the sentence "I am the network." To him, his being the network not only consists of his expertise in software engineering, but also his bringing together member states and convincing them to routinely share information.

5 Both the "briefing" with the project manager [hereafter cited as EUROSUR Project Manager at Frontex, personal interview (May 15, 2012)] and the follow-up telephone conversation [hereafter cited as EUROSUR Project Manager at Frontex, telephone interview (June 26, 2012)] required authorization by the Head of the Research and Development Unit at Frontex. Further communication via email also required authorization. Regarding several responses, concerning, for example, the usage of data and screenshots, authorization by the European Commission or the Head of Research and Development Unit at Frontex was required. Not all requests were granted.

"I have a long experience in international relations […]. And I know where the difficulties are. So instead of doing a big bang technical solution, because it is not technical, what I did when I arrived here – they asked me: 'You should work in the EUROSUR network.' And I say, 'Okay, I know how to do it.' I call the member states, and got them – three, four meetings – asking them: 'What information do you manage today that you *may* be willing to share with others?' And that is the starting point. And then I will give you the minimum technology to support that exchange, the minimum!"[6]

This statement can be quite surprising in that the system developer, and thus the main figure in terms of technical feasibility and implementation, states that "it is not technical." Moreover, despite political rhetoric's emphasis of EUROSUR as a "technical framework"[7] and the "system of systems,"[8] and despite being characterized as surveillance behemoth by critical commentators,[9] EUROSUR is presented as minimalistic in terms of its technological setup. Hence, a new question arises: What kinds of difficulties are located beyond technicality?

Judging by the objectives of EUROSUR – namely, increasing the interoperability of existing surveillance systems, information exchange, and situational awareness among border agencies in the EU – and taking seriously that these are not technical issues, the focus falls on the willingness, acceptance and compliance of EU member states to share information with each other and possibly with an institution at the supranational level of the EU. Subsequently, the legal discrepancies in terms of information policies turn out to be important. Regarding already existing formats of information exchange and data sharing between law enforcement agencies in the EU, such as the Schengen Information System (SIS), European Dactyloscopy (EURODAC), and the Visa Information System (VIS), Leon Hempel and colleagues note that "interactions become even more complicated at the transnational level of the EU: the cultural, social, organiza-

6 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

7 EUROSUR Roadmap, COM(2008) 68 final.

8 Ibid.

9 Initial reactions to the Commission's envisioning of EUROSUR focused on the type and amount of surveillance technology that could be connected to the system. Particularly the involvement of the arms industry and the number of FP7 projects mentioning EUROSUR as a possible "end user" initiated criticism. Often the amount of money spent in research and development has been taken as an indication of its being "big and bad." In this context, the term 'drones' was deployed as a controversial stimulus and a platform of critique (cf. Kasparek 2008; Tsianos 2009, Monroy 2011).

tional and legal differences between the data exchanging law enforcement authorities increase to a maximum of complexity" (Hempel/Carius/Ilten 2009: 5-6). In practical terms, this means that the exchange of information is hampered more by disharmony and a lack of trust between organizations (Balzacq/Hadfield 2012; Aden 2014) than by the incompatibility of the technical systems used by administrations. Generally, the exchange of information between law enforcement agencies – particularly the exchange of operational information – is a sensitive issue. A NATO press officer mentioned to me that European member states routinely refrain from sharing information rather than the other way around. Anecdotally, he noted that even the brand of toilet paper provided in ministries was treated as classified information. The general secrecy and non-disclosure claimed by administrations can be deployed as a means to keep control over one's own information and avoid being monitored from the outside.

Hempel et al. see the reluctance of some member states to exchange information as a "symbolic answer to the overall EU strategy of integrating national security policies at EU level, thereby consuming essential parts of national sovereignty" (Hempel/Carius/Ilten 2009: 10). In fact, a centralized technical system could allow unwanted control and comparability both between member states and between the states and the European Commission. Effectively, information exchange means that internal procedures become visible and hence subject to evaluation, comparison and, ultimately, control. Maintaining authority over one's own national information can be considered a strategic element against Europeanization. Moreover, exchanging information also requires compliance to a reporting format that might differ from national routines and thus cause extra work.

In order to eventually persuade member states to share information via the EUROSUR network, a bottom-up approach dominated the development phase during which all steps and propositions were carefully considered. This incrementalism is alluded to in the passage quoted above: "I call the member states, and got them, three, four meetings, asking them […]. And this is the starting point."[10] It becomes clear that convincing member states to listen to the proposal is hard work already. Creating the conditions for a starting point required "three, four meetings"[11] to mitigate skepticism and to make initial inquiries into the national status quo in terms of the availability of information and data.

10 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

11 Ibid.

Thus, the starting point has been to create a general inventory of the kind of information national border authorities collect in their institutions. The tentative phrasing of "information […] that you may be willing to share with others"[12] requires for principle willingness. Political, administrative and legal details – such as who will be entitled to request information, who will receive it, how much administrative effort or even restructuring will be needed, and how the information will be used – are set aside for the moment. By taking stock of the kind of information national authorities manage today, a list is made that assembles border-related information, which will then be further addressed.

4.1.1 Europeanization by Design: Defining and Designing "Border-Related Incidents"

As soon as a list is available, its content can be sorted, organized and categorized. Thus, according to the preliminary schema of the pilot phase, border-related incidents were to be grouped as either "illegal immigration," "crime," "crisis" or "other." The responsible project manager at Frontex (P.M.) described the genesis of the classificatory schema as follows:

P. M.: The first thing I created was a schema with four types of information and this schema is a tree that can be expanded or cut.

S.E.: And what kind of information is that?

P.M.: They [that is, the member states] say that they want to share information on illegal immigration, crime, crisis and other. […] I am using the information of the member states here. They say: "Crisis for us is: if there was a fire in the forest and we have to abandon the [border] crossing point, this is a crisis for us, or we are using a border guard helicopter to evacuate people from a boat. This is not illegal immigration and this is not crime, so crisis." So this is the starting point: "What do you want to share?" And I facilitate that in a system which is extensible, stretchable.

My interviewee describes a situation here in which representatives from member states have exemplified their operations and difficulties related to border policing, which they were asked to group and evaluate. At face value this can be un-

12 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

derstood as striving for a common heuristic ("this is crisis for us"[13]). Information-sharing has two requirements: it requires a principle willingness *and* a format that is understood and accepted by all participants. "You need to have common definitions," the Head of the Research and Development Unit at Frontex stressed, "because otherwise it is going to be a big mess." He explained:

"If somebody is considering this coming under this heading and somebody else considers this as being under another heading, and then the whole structure gets completely lost. So you have to have these common definitions before you can start developing any system like this."[14]

To achieve these two requirements, a classificatory schema needs to resonate both with the local (that is, individual) conditions of different national border authorities and with the global view of the European Commission. How things are named must thus be vague enough for all authorities to locate their issues while creating the impression of that they are represented correctly. They must also make sense in the context of a common task. The elements of such a classification must bridge and translate between the local and the global level, between national concern and European outlook. The classificatory schema for sorting border-related information that the project manager proposed to the representatives of the member states thus had to function as a "boundary object" (Star/Griesemer 1989) – that is, it had to be "both plastic enough to adapt to local needs […], yet robust enough to maintain a common identity across sites" (ibid: 393).[15] In the case of EUROSUR's classificatory schema, the challenge was that it had to first create (rather than maintain) this common identity, which member states were reluctant.

13 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

14 Head of Research and Development at Frontex, telephone interview (October 28, 2011).

15 Susan Star and James Griesemer identify four types of boundary objects: repositories, ideal types, coincident boundaries, and standardized forms. The characterization of coincident boundaries almost reads like a description of EUROSUR's functional raison d'être. They are "common objects which have the same boundaries but different internal contents. They arise in the presence of different means of aggregating data and when work is distributed over a large-scale geographic area" (Star/Griesemer 1989: 410-411).

Ultimately, the question of how to reach an agreement regarding adequate titles is centrally related to the communication of local events under a common European heading. Apart from streamlining understanding, it also concerns prioritizing issues according to relevance for the shared responsibility of Schengen borders. This is because discussing the meaning of different types of border-related information inevitably triggers a discussion on the critical point when a local phenomenon becomes an issue that should be considered a problem for the entire Schengen area. Thereby, claims and complaints by individual member states are put into comparison and hence into (a European) perspective.

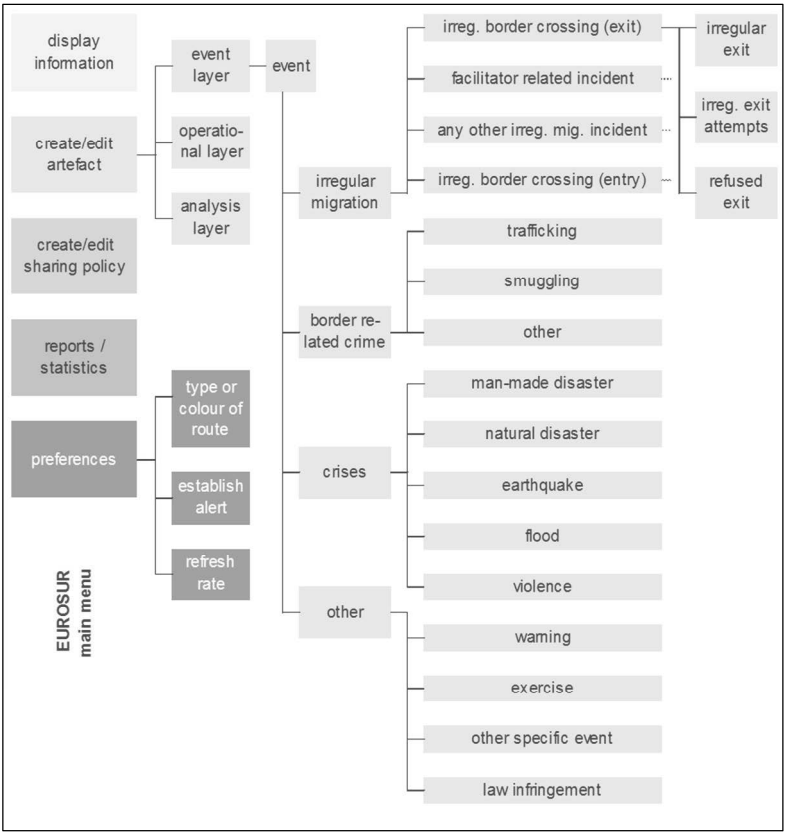
The search for common definitions prepares and, if successful, also supports the formalization of information exchange. However, there is more at stake than formalization. In their study on the creation of information infrastructures and the role of categories therein, Geoffrey Bowker and Susan Star stress that "[s]eemingly purely technical issues like how to name things […] in fact constitute much of human interaction and much of what we come to know as natural" (Bowker/Star 2000: 326). In this sense, the EUROSUR on the screen and the menu bar of its graphical user interface provide a new way of looking at the border, while also proposing a mode of naturally recognizing the external border of the EU as emerging from events, issues and trends of concern. In order to reify and naturalize EUROSUR's classificatory schema, its defined types of border-related incidents are reformulated as: (a) *technical* – which in this case means as *digital* menu items, (b) *iconographic* – they are represented as icons, and (c) *legal* – they are fleshed out in the regulation as a sub-layer of events and are partially furnished with examples. Consequently, border-related incidents appear as menu items and graphical icons on the graphical user interface (GUI) and as sub-layers of the events layer as in the software architecture of the GIS and in the legislation. In this way, the common definition of types of border-related information is successively stabilized.

Technical Framework: Border-Related Incidents as Menu Items

When the test-application was shown to me in May 2012, the schema was already part of the menu bar. By transforming the schema of four types of information into menu items, it became the first element in the infrastructure of the EUROSUR network. The schema was thus transformed from a loose question of "Under which heading would you communicate your event?" to an IT item that is materially available, selectable and clickable. Moreover, different types of border-related incidents were identified and proposed by the national coordination centers (NCCs) of member states participating in the test phase.

This resulted in a series of items in the menu bar and the so-called "incident catalogue," an inventory of all incidents relevant for the common enforcement of the external EU borders.[16]

Figure 5: Catalogue of "border-related" incidents" in the test application



Source: own reconstruction, designed by Nils Ellebrecht

16 Up to today, the incident catalogue is subject to constant adjustment, and is not officially in the public domain. As these incidents sort out events relevant to border control, the process of defining them illustrates a European consensus about what is regarded border criminality, despite of the absence of a common EU immigration and asylum law.

During the pilot phase, participating member states could assess whether the schema was working in practice and how it could be amended and differentiated. As a result, two capabilities were tested in the pilot phase: fitting the classificatory schema with the views, needs and interests of the participating member states, and the usability of the IT application. For participants, testing the application included getting used to a certain way of looking at the border and of perceiving information as border-relevant.

This customization is supported by the interactive features of the platform that allows the user to both enter and retrieve information. The user can also filter the information by navigating the menu items to select certain types of incidents. They will then receive a map on, for instance, cross-border crime. Similarly, when a user intends to input information into the system, they are asked to select from the different types of border-related incidents and to classify the information according to this agreed schema. In the meantime, both the application and the schema remained flexible; the system is "extensible, stretchable"[17] and can also be reduced. This certainly evokes an atmosphere of "playing around" with the EUROSUR network in a non-binding way. Thus, rather than participating in new intergovernmental or communitarian obligations, the personnel at the NCCs became used to interacting in an electronic network. Rather than discussing common policy objectives or programs, member state representatives discussed menu items.

Iconographic Framework: Border-Related Incidents as Icons

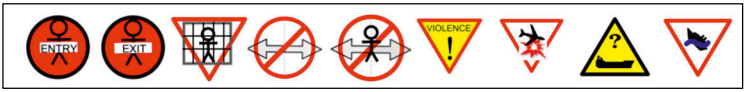
All border-related incidents are rendered commensurable by way of icons. This has effects on both cartography and organization. Each type of incident has an assigned icon (cp. figure 6).[18] The fact that the different icons have been designed to imitate traffic signs[19] – and hence appear mainly in red and yellow with a round or triangular shape – alludes to a self-image of border policing as the regulation of movement and traffic. The protection of borders has thus been transformed into the control of routes and entry points.

17 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

18 As an anecdote, it is interesting to mention that, when I was at the network office, the icon for a stolen car had just been developed after the Eastern authorities requested it be a border-related crime. In addition, the ability to delete messages was added during the pilot phase, when there was also a monthly update of the application.

19 Head of Research and Development at Frontex, telephone interview (October 28, 2011).

Figure 6: EUROSUR Icon Examples



Source: "EUROSUR: The Pilot," presentation slide[20]

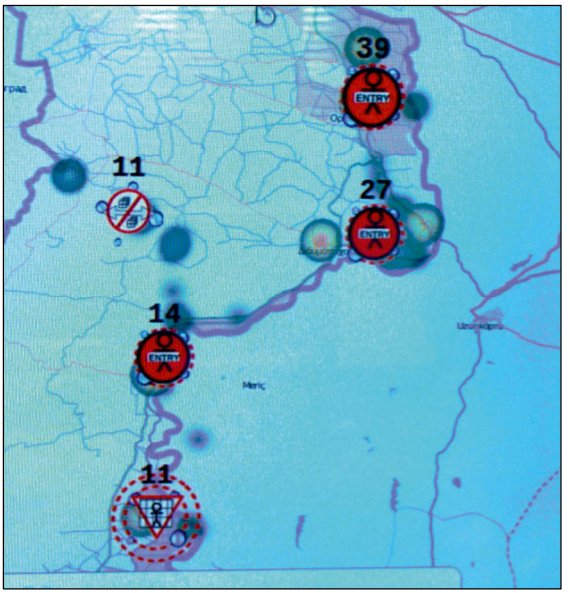
The translation of the type of incident into an icon visually condenses the information, thus reducing the material for the part of the electronic map in question. The icons are placed according to where the incident has occurred. If a series of events are reported in a single area, the red icon is surrounded by blue circles, which is meant to attract the operator's attention. In addition, the current number of incidents at a particular spot is indicated in bold numbers on top of the incident icon. The operator can drag the cursor over the icon to display the individual events and to select the respective incident report. In practical terms of information exchange between border agencies in the EU, the icons bridge existing language gaps: While the EUROSUR network is set up in English, it is not the working language in most national offices.

The common iconographic language may therefore be able to compensate for potential communication difficulties. Apart from these language barriers, icons are also able to bridge diverging interpretations of issues and even work when common definitions have not yet been fully achieved. They even out incongruences and national divergences. They approximate understanding without consensus by offering the flexibility to apply individual perspectives and fill a common icon with individual examples. They embody the quality of boundary objects.

The semantic interoperability offered by icons suggests a common understanding, even when its content is still contested. The icons thus facilitate usability, and they visually offer and anticipate a consensus even before it has been reached. Moreover, the symbolism of traffic signs suggests that there are set rules for movement in Europe. Finally, by way of accumulating events, the necessity to act seems obvious when looking at the map.

20 Gregorio Ameyugo Catalán (Frontex): "EUROSUR. The Pilot," presentation during the European Day for Border Guards at the Frontex Headquarter on May 24, 2010 in Warsaw, Poland, at: http://www.ed4bg.eu/files/files/ Ameyugo_FRONTEX.pdf (accessed September 28, 2011), here slide 10. (Repository S. Ellebrecht)

Figure 7: Mapping border-related events



Source: own photograph, taken in May 2012, revised in color

Legal Framework: Border-Related Incidents as "Sub-Layers" of the "Event Layer"

The consensus on the kind of information to be shared and on how to sort it has been addressed in the EUROSUR legislative proposal of December 12, 2011[21] and fixed in the EUROSUR Regulation of October 22, 2013.

In the latter, the different types of information are circumscribed as "sub-layers" of the "events layer." Article 9 (3a-d) of the EUROSUR Regulation states:

21 European Commission (2011): Proposal for a regulation of the European Parliament and of the Council – Establishing the European Border Surveillance system (EUROSUR), COM(2011) 873 final (December 12, 2011) [hereafter cited as "EUROSUR draft regulation" or "EUROSUR legislative proposal" COM(2011) 873].

"The events layer of the national situational picture shall consist of the following sub-layers:

(a) a sub-layer on unauthorised border crossings, including information available to the national coordination centre on incidents relating to a risk to the lives of migrants;
(b) a sub-layer on cross-border crime;
(c) a sub-layer on crisis situations;
(d) a sub-layer on other events, which contains information on unidentified and suspect vehicles, vessels and other craft and persons present at, along or in the proximity of, the external borders of the Member State concerned, as well as any other event which may have a significant impact on the control of the external borders."

At this point, it becomes clear that the regulation largely describes the software architecture of a geographic information system (GIS). It is, however, remarkable that the regulation does not list the full number of border-related incidents to be communicated – that is, that is does not provide an incident catalogue. The technical option of selecting items from a menu translates in the regulation into an information request and hence as "the national situational picture *shall* consist"[22] of these types of information. At this point, playing around with a test application becomes an obligation to communicate certain things in a certain way under defined headings. Thus, the inventory of border-related information has been transformed from a list into a classificatory schema of four types, a selection option in a menu bar, and finally a request for a particular kind of information.

Bowker and Star aptly emphasized that classifications "are powerful technologies. Embedded in working infrastructures they become relatively invisible without losing any of that power" (Bowker/Star 2000: 255). Indeed, the EUROSUR network offers a new working infrastructure, which in turn produces a new perspective on the task of border management. The process of establishing a working infrastructure for the exchange of information that is acquired and integrated into the relations between border authorities seems to weigh more than the content of the information itself.

22 EUROSUR Regulation (EU) No 1052/2013, Art. 9 (3a-d), emphasis added.

P.M.: I used to use this anecdote, this metaphor: this system is the train system, the station, the train, the trucks, but the cargo and the passengers is an issue for you, the users. So, I provide you with a secure train system; cargo and passengers are up to you.

S.E.: It is a huge system.

P.M.: In fact, it is small. Look at this; this will sound philosophical, but look, this network that I have created is using the minimum technology because I know that technology is not the issue. And the application may change, the security of the network may change, the network itself may change, it could be a dedicated network in the future; but what should be permanent is the community of people that are getting used to sharing information; that part should be permanent, and how they do it. We have a super solution now that may evolve and may change.[23]

The border-related incidents (whether as menu items, icons or sub-layers) are offered as a new convenient way of judging and sorting what is happening at the border. They are proposed as *wagons* of the "secure train system" to transport information. However, even though presented as intermediary, the classificatory schema of border-related incidents does not simply *transport* information. It mediates a new way of perceiving the external border of the EU. It is therefore worth stressing that the entire process successfully continued without defining "border-related." The monopoly of interpretation lies in the act of visualizing information on the EUROSUR electronic map. What makes it onto the map becomes relevant for common border policies.

4.1.2 Sorting, Reporting and Evaluating Information

Having developed a classificatory schema to sort border-related information, member states were asked to report events using the different headings available on the GUI. Generally, occurrence reports are an essential part of police work; internally, they fulfill the function of documentation and accountability. Furthermore, they can be used as pieces of information to be forwarded to other institutions. When information is forwarded among several institutions, as in the EUROSUR network, further agreements are required, concerning:

23 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

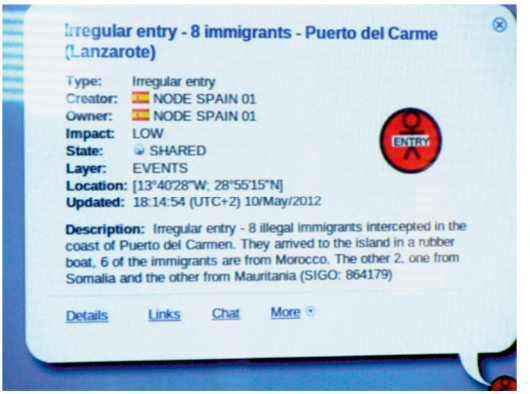
- the format of the report,
- the degree of automatization of sending information,
- the selection of information based on one's own preferences for or against sharing,
- the selection of information based on its relevance to the common border.

During the test phase, participating member states used the preliminary format of an incident report. The decisions regarding the degree of automatization and the selection of information to be forwarded in the network were left to the individual member states, whose representatives could "play" with the system. It is important to stress that the incident report as displayed in the photograph in figure 8 shows the version that was available in May 2012, which has most likely since been updated. It shows the format in the test phase that provided several features that are no longer part of the application description in the EUROSUR Regulation. The value of presenting and discussing the format anyway lies in the fact that significant aspects that fostered the compliance of member states with the EUROSUR network can be demonstrated in this test version. It shows that different material development steps are not merely incomplete stages of the end product; they are seminal mediators that provide of the potential for further acceptance and development. Accordingly, they resemble those "fragments of the story" which Michel de Certeau recognized in the sailing ship painted on the sea, indicating "the maritime expedition that made it possible to represent the coastlines" (Certeau 2013 [1984]: 121). Although the sailing ships become invisible through the transformation of the depiction of coastlines into maps, they represent and call to mind the operations from which the map resulted.

Incident Reports

In the frame of the EUROSUR network, incident reports can be considered the basic format of information exchange between member states. Border-related incidents are entered into the system by clicking on the pencil icon, which is called the "artifact editor." In the language of EUROSUR users, the occurrence is then transformed into an "artifact." A so-called "new artifact" consists of the following nine details, which the artifact editor requests in an input mask: type, creator, owner, impact, state, layer, location, updated, and description. To enter an incident report, these boxes must be filled in.

Figure 8: Reporting incidents from the border



Source: own photograph, taken in May 2012, revised in color

These reports on events can be published on the national situational pictures (NSP) of the reporting member state, meaning they remain with that member state, or they can be forwarded to selected partners and also appear on their maps. When published on the electronic map; incident reports are represented by different icons, as described above. If we click on an icon, a file card pops up in the shape of a speech bubble, displaying the information that has been filled in the boxes (see figure 8). Given the fact that the communication format of the incident report structures both the reporting and the reception of the information on "border-related" events, it is worth discussing its different elements.

In the "artifact editor," the author selects a "type" of "border-related incident" from the menu. The classification of the incident also appears in text format in the first line of the file card as "type." Figure 8 provides an example of an incident report for an "irregular entry." The respective icon, placed on the top right side of the file card, repeats the type. This again underlines the importance of the iconographic translation of the classification: The graphical image, the "traffic sign," supports the standardization of common definitions, as it translates particular events into icons of common concern. Moreover, the last box at the bottom of the speech bubble asks for a "description" to accompany the information on the reported event.

This means that the sorting is illustrated, and the classification is performed and customized. Moreover, other participants are able to see whether a respective heading has been chosen appropriately. These three boxes – type (selected from the menu bar), icon (which visualizes the incident accordingly) and description – support the customization of incidents to the classificatory schema through paraphrasing.

The next five boxes negotiate the issues of ownership and authority over information and data. The first two boxes distinguish the "creator" from the "owner" of information. With regard to the information provided by member states, the owner of the information is identical with the creator of an incident report. However, the "owner" of information could also be a source or party who is not part of the EUROSUR network, but who provides information on agreement. Information regarding vessel traffic, for instance, might be provided and owned by EMSA. In this case, the creator of the information in the EUROSUR network would, however, be Frontex. Likewise, Frontex might be the "creator of information" during Joint Operations (JOs), while the "owner of the information" would be the host country. According to the terms of use, any participating national coordination center (NCC) – or in the language of EUROSUR, every users or node – could be the creator of information. Frontex is also a node, yet it lacks the mandate of an investigative authority. However, in the interactive setup of the IT application, the entry of information is not bound to the rights of that information or data. In the case of the EUROSUR network, it could thus happen that Frontex, although not allotted an investigative mandate, can create information relevant to the operationalization of border policies. The standard in information security, according to which an institution which creates and stores information is the initial owner of that information,[24] is thus made flexible. Moreover, the distinction between owner and creator might become increasingly sensitive when it comes to operational information: will a Maltese border guard be allowed to report something he sees in the Italian waters to Frontex and vice versa? Does reporting imply operational obligations? Who creates information during a joint operation? And is reporting different from being responsible?

The labeling of a participant as the "owner" of information demonstrates a signaling effect toward member states, in the sense that their sovereignty is documented by being named the owner of the information in the reporting system, but the legal framework of informational sovereignty is unsettled by the very distinction between the creator and the owner of information. As a node, Frontex can create information without having the rights to generate surveillance information itself. The lack of sovereign competence is compensated for by referring to the "owner."

24 Information Security Glossary, sub voce "Information Owner," at: http://www.yourwindow.to/information-security/gl_informationowner.htm (accessed August 7, 2019).

The next three boxes – "impact," "state" and "layer" – further interfere with the setup of the ownership of information by relating the assessment of information to the way it should be treated and shared in the network.

The "impact" refers to the assignment of an "indicative impact level," which ranges from "high" to "medium" to "low." During the test phase, only those incident reports were requested to be sent to Frontex that had been assigned a medium or high impact level, while low impact reports were kept at the NCCs. This offered them the possibility to use the system without exchanging all of the information all of the time. Additionally, the box "state" indicates whether the information in the incident report is to be kept "closed" (that is, with the NCC) or whether it is to be "shared" with other network participants. During the test phase only, it was possible for member states to decide what information they wanted to share with what other participants.

The box "layer" sorts different kinds of information and offers the following options: "events layer," "analysis layer" and "operational layer." All three layers reveal and negotiate the tension between local issues and the assessment of their relevance for common European border policies. Considering member states' strong reluctance to exchange information on national procedures and events, and thereby disclose it to a European view, the processes during the test phase were intended to demonstrate that local events are part of a bigger picture (materialized in the ESP) and that there was therefore a "responsibility to share."[25] However, while filling in information, operators did not necessarily apply a European perspective, but were also selective and influenced by national interests. For instance, local occurrences that have been dramatized and assigned a high impact level may suggest (that is, create evidence for) a desire for more funding. Conversely, controversial or low-standard operational practices could be hidden in the system by assigning them a low impact status (or simply by not reporting them at all). The following two sections will describe these temporary conces-

25 Jargon among officials at the European Commission and Frontex responsible for the EUROSUR development phase (December 2012). The official jargon changed here from "need to know" and "need to share," to "responsibility to share." Effectively, these formulations take a step back from the principle of availability and its demand toward member states to provide information without further ado (cf. Bunyan 2006; Töpfer 2008). Moreover, the principle of availability refers to criminal law information, which are not addressed in the EUROSUR GUI. Again, it shows that EUROSUR has not been developed along existing legal categories, but makes its own definition offer.

sions and compare this procedure with the final rule in the EUROSUR Regulation.

First, however, it should be mentioned that the details on space and time ("location" and "updated") provided in the incident report allows us to deduce the possibilities and motives of the EUROSUR network in terms of a timely operational response. Although information on the "location" indicated with longitude and latitude coordinates can be relevant for operational decisions as well as for the retrospective transparency of events, it is useless when reported one day after the occurrence. Yet, the time tag does not ask for the time of occurrence, but rather refers to the information in the incident report, stating when it was last updated. This documents when the incident became an artifact in the system, or when the information was changed. The continual possibility to update e the incident report lets the EUROSUR seem more like a documentation platform and archive than as an agency supporting prompt interventions. In fact, Martina Tazzioli, who in 2014 had the chance to conduct ethnographic work in the Italian NCC after EUROSUR became operational, found that "the average time of latency between a migration event being added to a map and being displayed is of some hours and can reach two days" (Tazzioli/Walters 2016: 9). Apparently, this has not changed much since the pilot phase, when it was considered a success by Frontex and EC officials if "the stuff is inside the system within 24 hours."[26] Compliance with and the actual usage of the system is thus critical for any evaluation of EUROSUR's function as an agency supporting operational reactions.

I will now return to those temporary concessions that fostered the compliance of member states during the pilot phase and initially allowed them to maintain control over their national information.

Sharing Policies: Maintaining Control Over One's National Information

Since the EUROSUR Regulation of 22 October 2013, all incident reports created in the IT network are sent to Frontex. While some NNCs can automatically retrieve the information, most participants enter the information manually, although the exchange of information is instituted and regulated via the EUROSUR system. For some, this high level of compliance may come as a surprise.

A look at the test phase demonstrates the gradual process of convincing member states and getting them to share information and become less reluctant toward a European standard format of communication regarding operational in-

26 Formulation used by an EC official in December 2012.

formation. When I interviewed the project manager responsible at Frontex during the test phase, he described the options for the exchange of information in the following way:

S.E.: Does one have the opportunity to select the information that will go into the network?

P.M.: There is the option of selecting between automatically or manually. But first, when you inject information in the system, it is injected locally, because maybe your people want to see it and maybe you want to discuss this with other people in the NCC. And then someone has to publish it. And when you publish, the information will be distributed following the sharing policies that you have established.

S.E.: And what could be the sharing policies?

P.M.: Sharing policies are defined by each node [that is, NCC]. For instance, illegal immigration will go to everybody, crime will go to France and Italy, crisis will go to everybody, so this is the sharing policy.[27]

The option to define individual information sharing policies was crucial to the acceptance of the system among member state authorities. Member states thus maintained authority over their national 'border-related information' in two ways: First, national authorities decided which information would be shared with whom – that is, the participants could exploit the system to their advantage and interests without having to comply with a central demand to provide information. A selective usage of the system was allowed; there were no strings attached, just strings of digital references were offered. Second, national border enforcement activities were not reported on the European level, which essentially would have suggested a central supervision of Schengen activities. When asked whether these different options were part of the design from the beginning, the Frontex official replied at length:

"I planned it in this way, after discussion with the member states. I got their answers, and I quickly saw that they didn't want to have a big brother. I saw also that if we establish a centralized system, the centralized system will be managing the information which will be

27 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

the common denominator of everybody. And that common denominator will be very small, so 'No thank you' – we will not have a centralized system."[28]

The obstacles to sharing information are identified as conflicting interests and fear of supervision. Convincing member states to loosen their sovereign monopoly over national surveillance information and to routinely and actively share information required added value. For, if the common denominator is "very small" and members' reluctance to report their own activities is great, the system will not take off. The Frontex official describes a kind of skepticism that is typical for law enforcement agencies with regard to the exchange of information: the belief, or rather concern, "that communications amalgamation breaks down both territorial and formal organizational boundaries" (Ericson/Haggerty 1997: 393). Hence, the EUROSUR system was explicitly offered to member states as a service in which each participant could select the options that best benefitted their needs.

"We have a distributed system with the possibility to create communities of interest. And if there is one of the nodes that cannot see some type of information – so what? This node will not see it. But the others – why not?! You may create a community! Imagine that we're having 25 nodes, and there are five nodes that have customs' information – because this picture of the NCC having all the information is not real – so imagine that there are five that have customs information, and they are able to share that information between them. We will be helping them! And that will be part of their border situation, and they will have a European situational picture of their region that will be richer than that of other nodes."[29]

Future additional reporting burdens were left to the member states to decide. The incentive to do so, however, was established with reference to the value of information itself: "If I am very active and if I am sharing a lot of information with the others I will have a very rich map, so if I am very active, I will have a rich map."[30] A glance at the EUROSUR electronic map shows why this circular argument could be convincing. Engaging in the exchange of information, and sharing a great amount of information with many partners meant having more tags on one's own situational picture.

28 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

29 Ibid.

30 Ibid.

Getting involved was visually rewarded with a "richer map" and the feeling of knowing what was going on at the common borders. Again, the option to define individual sharing policies was crucial to the acceptance of the system by member state authorities. Still, the idea of generating different national pictures of the situation at the external borders was not in the interest of the European Commission, and ultimately sharing policies disappeared with the publication of the final regulation.

Impact Levels: The Traffic Lights of Border Control

In addition to reporting occurrences in the form of an incident report, NCCs are requested to assign each incident an "indicative impact level, ranging from 'low' and 'medium' to 'high.'" The purpose of this procedure is primarily to assess local events with regard to their relevance for common Schengen border policies. What local occurrences weigh enough to impact Schengen responsibilities? Put differently: What local information is also relevant to others, and to what extent? In this case, "impact" is not further defined, as this could be construed as being overly demanding and perhaps even patronizing toward member states who may then no longer accept the system and could leave the test phase.

During the test phase, the assignment of impact levels was monitored by Frontex. The agency ran a so-called "consistency check" on how member states apply the impact levels. However, this consistency check had the potential to go beyond this information submitted with the incident report and to additionally enable national claims to be put into perspective. "It is not just exchange of information," noted a Frontex official, "it is also asking for information and asking the Italians: 'Why do you think that this event is high impact when we see that it is only related to a single Moroccan?'"[31] The impact level thus not only reports local urgency, but also allows for comparability. The application of impact levels can thus be considered a relatively strong insight into national affairs and border police work, and its acceptance by member states therefore surprising.

As already mentioned, this acceptance emerged gradually. During the pilot phase, the value of these procedures could be tested without having to share all of the information all of the time with all of the nodes. In fact, those events assigned a low impact were intended to remain in the member states' NCCs. Medium and high impact incidents were sent to Frontex where the "consistency check" was applied. Assigning a low impact level to an incident thus meant keeping control over the distribution of an incident report. In this sense, the rule

31 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

that incidents of low impact need not be shared with Frontex did not necessarily mean that the incidents were of minor importance to overall European border management, but rather allowed member states to be active in the system *without* being monitored by others. That the draft regulation proposed that "[a]ll [read: only] events assigned with a 'medium' to 'high' impact level shall be shared with the Agency"[32] can be regarded as the top-down expectation of the European Commission to at least routinely share those incidents with Frontex that member states considered as having a moderate or significant impact on the situation at the common external borders.

However, the final regulation no longer grants the selective exchange of information, but rather prescribes that *every* incident "shall be shared with the Agency."[33] This can be judged as a positive achievement of the European Commission, which was able to convince the Council that all incident-reports go to Frontex.

"The argument on the side of the Commission in this regard – and the member agreed – was: if a migratory route is altered and a new route is being tested, it is not risked [by facilitators, S.E.] to send 30, 40 or 100 persons which then are intercepted. Rather one sends three, five, ten persons and it is watched how permeable the border is; now, these incidents would be classified as low impact. But if one was already able to *see* these incidents, new routes could be detected much faster, instead of waiting until member states report these 30, 40 or 100 persons. "[34]

Finally, the EUROSUR Regulation requires Frontex to "visualise the impact levels attributed to the external borders in the European situational picture"[35]. For this purpose, Frontex aggregates the individual impact levels in the context of the agency's risk analysis, referring both to the impact level assigned by member states and the frequency of incidents of a specific type along a defined "border section." This visualization consists of the respective border section being colored, so that different parts or dots along the external borders of the EU appear as green, yellow, or red stripes.

32 EUROSUR legislative proposal COM(2011) 873, Art. 9 (4).

33 EUROSUR Regulation (EU) No 1052/2013, Art. 9 (4).

34 EC official in Brussels, personal interview (December 2012).

35 EUROSUR Regulation (EU) No 1052/2013, Art. 15 (3).

Figure 9: Frontex's demonstration of border sections and impact levels

Source: European Commission, press release of November 29, 2013[36]

This means that the distinguishing aspect of an incident is no longer the national border, but the color-coded impact level. Additionally, the color codes are not applied to national borders, but to designated border sections. The EUROSUR Regulation requires each member state to "divide its external land and sea borders into border sections, and […] notify them to the Agency"[37].

Border Guard Major Świąteka reasons that national borders would be too general a unit, as "it depends on what is happening on the other side of the border."[38] Furthermore, she considers the assignment of impact levels more of an exercise of semantic interoperability. During a presentation on EUROSUR, she stated: "It is not just to give names; we will be obliged to react accordingly. This is why EUROSUR is not just a system for the exchange of information but

36 European Commission (2013): EUROSUR: Protecting the Schengen external borders - protecting migrants' lives, MEMO/13/1070 (November 29, 2013), p. 3, at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_13_1070/MEMO_13_1070_EN.pdf (accessed August 15, 2019).

37 EUROSUR Regulation (EU) No 1052/2013, Art. 14.

38 BG Major Świąteka: EUROSUR Presentation (May 16, 2012).

much, much more."[39] Even if the authority of border guards is still tied to territorial borders, as depicted on the screen, their place of operation is denationalized and dynamic.

Coloring puts the self-evaluations of the member states into a supranational perspective. This allows for comparisons, while also painting a new picture of the border: no longer are state borders drawn as lines on a map, now their insecurities are identified, aggregated, and visualized as concerns rendered in color. While this new outlook affects the image of a common EU border, it is also referred to for the allocation of resources and personnel, as the EUROSUR Regulation foresees "reaction corresponding to impact levels."[40] Thus, in the process of collecting, evaluating, aggregating, visualizing and coloring pieces of information, they turn into occasions or even evidence for intervention. According to the "EUROSUR on the screen," there is always something to do: perhaps more here (red), and less there (green). In this sense, the exchange of information fuses with the suggestion of operational urgency.

Layers: System Architecture and Techno-Political Filter

The division of the EUROSUR GIS into layers surpasses the conventional use of layers in a geographical information system. Generally, data on the distribution and characteristics of defined aspects are clustered into layers to be selected for display. This is also used in the context of EUROSUR when types of border-related incidents appear as layers or sub-layers, as described above. The practical reason for layers in the GIS is that it creates the possibility to select and combine information, or to single out a single aspect for display. This is also possible with the EUROSUR application. An operator can thus select "cross-border crime" and receive a map that displays only this defined information.

Additionally, it is interesting to note that the EUROSUR layers also imply different fields of responsibility. In addition to these thematic variables, which can be displayed layer by layer, the institutional structure of sharing and processing information via the EUROSUR network is also organized in layers. The Head of Research and Development explained this during the test phase:

"The way the EUROSUR network is built up is that we will have different layers, the operational layer, and the analytical layer, which can be used by different people. For instance, if you talk about analysis, you do not want operational people to have direct access

39 BG Major Świąteka: EUROSUR Presentation (May 16, 2012).

40 EUROSUR Regulation (EU) No 1052/2013, Art. 16.

to that layer. I mean this is a layer which is used for analytical people to compile information, to draw conclusions, basically, to do analyses. And this analysis will then appear in the network of EUROSUR. And if we're talking about the operational information, which is real time or near real time, this is the event or incident layer, as we call it, and this is where people, this kind of operational people, can put on things that are actually happening at the extern al border right now. So we see it in these kinds of layers."[41]

The layers the official is describing here distinguish competences and thus operate as protected spaces in the system. Moreover, these layers do not cluster information in terms of content, but in terms of how it is obtained and processed and according to its weight in knowledge production. Louise Amoore received a similar statement from an interview with a border security software designer in 2009. Her interviewee stated: "There is real time decision making, and then the offline team who run the analytics and work out the best set of rules" (Amoore 2011: 25). This new distinction in competences has thus been built into the IT architecture of EUROSUR by way of "layers." The draft regulation specifies the three layers with regard to the information they collect and in turn provide:

(a) an events layer, containing information on incidents concerning irregular migration, cross-border crime and crisis situations;
(b) an operational layer, containing information on the status and position of own assets, areas of operation and environmental information;
(c) an analysis-layer, containing strategic information, analytical products, intelligence as well as imagery and geo-data.[42]

The final regulation, however, merely lists the three layers that make up any situational picture in the EUROSUR: the events layer, the operational layer, and the analysis layer.[43] The wording follows the formal logic of a GIS. When the regulation was passed, customizing the participants to fit the distribution of tasks and competences in the EUROSUR network was no longer debated, but taken for granted. It no longer needed to be specified, as it logically emerged from the system. It is an *infra*structure that is taken for granted.

41 Head of Research and Development at Frontex, telephone interview (October 28, 2011).

42 EUROSUR legislative proposal, COM(2011) 873 final, Art. 8 (2).

43 EUROSUR Regulation (EU) No 1052/2013, Art. 8 (2).

In sum, discussing the EUROSUR network initially meant developing an IT application and discussing the menu options of its graphical user interface (GUI). The development of EUROSUR focused on what this could look like and how it could be represented on a screen. Different national angles were tentatively subsumed under menu items, domains of responsibility were translated into GIS layers, and organizational hierarchies were flattened into nodes in the system. Regarding the test application, discussions were geared toward (and reduced to) the GUI, the usability of which mediated the negotiations. To a certain extent, a question of sovereign competences (in this case, the authority of one's own national information) was flanked by, reduced to or even smothered by the question of software design. Ultimately, it can be assumed that it was most likely easier to get used to menu items for the purpose of testing an IT application than to agree on common priorities for border policies in Europe. Because interaction is mainly with the platform rather than member states engaging in discussions, the exchange of information ensues smoothly. Or, as Ruben Andersson commented pointedly: "If they started talking, it would never happen" (Andersson 2016: 13).[44]

In effect, the fact that officials did not want to make these development steps public because they said that they were "premature" highlights the frailty of the inter-organizational agreement at this time rather than the technical shortcomings. What was critical about the pilot phase was not the readiness of the technology, but the compliance of the member states.

4.2 THE EUROPEAN SITUATIONAL PICTURE

The immediate purpose of the exchange of information in the EUROSUR network is the generation of the European situational picture (ESP). Frontex provides the ESP to the national authorities active in national coordination centers (NCCs) in the format of the electronic map described above. During the pilot

44 From the quoted passages in Andersson's essay; I assume that he had the same interview partner as I did. Certain formulations are very similar to the statements I recorded. This demonstrates nicely that Frontex officials not only "brief" social scientists (cf. fn. 4 and 5), but are themselves briefed. Certain formulations seem to be deliberately released to the public, as if their effect was expected. Dealing with the controlled disclosure of information limits ethnographic work in the (border) security domain more than dealing with difficulties acquiring access or finding interview partners.

phase, member states experienced the added value of sharing and accumulating their information by seeing it all assembled in the European situational picture. This visualization literary makes visible the added value of exchanging information, which is in turn accessible as an object and thus exploitable by participants. This having been said, the EUROSUR electronic map is about Europe's borders. Geographic features are secondary in the cartographic representation and can be changed by the individual user, that is, by each NCC. "The map is a holder of information," explains the responsible project manager at Frontex, who argued:

"We don't need to have very precise maps because we just use them as a place holder for the information. Nevertheless, in the rack that I am installing, there is one server of maps. We are providing three maps, but if one of the users wants to put their own maps, they can do it."[45]

As the official said about the test phase of the network, the background map's "open street layer," which appears by default – presenting a white European continent in front of a light blue background (figure 4) – was never changed by member states. The reason was obvious to him: "Then the events are more visible."[46] In fact, the ESP is all about the visibility and tagging of events,[47] rather than the definition of a territory. While in the territorial frame the *drawing of a*

45 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012). – The "server of maps" offers three maps to choose from; apart from the one selected in the Frontex office, which in the system is called "open street layer," two further options exist – termed "blue marble" and "land set" – both of which are based on satellite images. The user has the possibility to manually select further configurations. Apart from the background map, it is possible to define whether bio-physical conditions should be indicated: forests, for example, can be added and would appear in green imitating biophysical appearances according to their actual color (cf. Ehrensvärd 1987: 131). The blue color representing the Mediterranean Sea is most likely also taken from the realistic tradition of imitating perception, which has been customized to the extent that it is common to talk about blue borders.

46 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

47 Martina Tazzioli also highlights the focus on events articulated on the map and describe this gaze as an "epistemology of the event" (Tazzioli 2018: 6). Joseph Pugliese argues that the "incident-as-event is the non-normative figure that ruptures the banal unfolding of normative seriality on the screen" (Pugliese 2014: 580).

single line allowed things and people to be organized, the *accumulation* of information, as in the ESP, lets single events that are suspicious to be identified or detected against the background of data. The ESP maps insecurities, hotspots of migratory pressure, and risks as they culminate into an accumulation of incidents marked as traffic signs or colored-in border sections. In fact, the ESP is not intended to provide a cartographic representation in which territorial border lines compartmentalize, contour and identify political authority; it was meant to provide a "situational picture" that can be used by authorities to develop operational strategies. Yet, what are the peculiar characteristics of a situational picture? What does its map accomplish? What is the argument its map is trying to make?

Situational pictures can quite generally be described as tools for making decisions. They arrange information as objects of concern that represent the spatial distribution of, for instance, adversary troops in the battle field, a certain type of crime, HIV or aids, or consumer patterns on a neighborhood, country or global scale. This can be arranged above a table or in a GIS-generated map to create a dynamic depiction of an object or theme in a defined area. The purpose is to produce an overview, a panorama, with regard to the extent and distribution of a defined issue of concern, so that personnel and resources can be deployed accordingly. In the context of inter-organizational cooperation, situational pictures also provide a platform for collecting information from different actors. Situational pictures can also be used to anticipate future developments or to trace the evolution of a situation. They are a typical asset in control rooms of all kinds, where they may be wall-sized or available on different screens. In any case, contemplating the picture is expected to lead to an informed, evidence-based decision that is tailored to the situation being viewed from a distance.

EUROSUR's definition of a "situational picture" states that the picture must be represented and accessible via ICT as a "graphical interface."[48] Its content is defined as "near real time data and information received from different authorities, sensors, platforms and other sources."[49] This surveillance data is visualized as a situational picture 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."[50] What is missing is any mention of the issue being displayed in the ESP.

48 EUROSUR Regulation (EU) No 1052/2013, Art. 3(d).

49 Ibid.

50 Ibid.

The definition merely answers Wood's and Fels's call for a definition of the map's performance and its argument by stating the purpose of EUROSUR's situational picture as achieving "situational awareness" and supporting "the reaction capability along the external borders and the pre-frontier area"[51]. The electronic map thus embodies a widely accepted rationale that there is a virtual causal relation between the availability of information and the effectiveness of (border) policing. It assumes that authorities know (or rather see) what to do. And the argument? What argument does the ESP put forth and on the basis of what supporting documentation? Judging from the Regulation's defined aim of "situational awareness" and its respective definition as "the ability to monitor, detect, identify, track and understand illegal cross-border activities in order to find reasoned grounds for reaction measures on the basis of combining new information with existing knowledge, and to be better able to reduce loss of lives of migrants at, along or in the proximity of, the external borders,"[52] the ESP is meant to argue ("find reasoned grounds") for reaction measures.

In effect, the non-representational map of the ESP argues that certain situations, such as a high-impact, red border section or an accumulation of incidents of a certain type require reaction measures. However, these reaction measures are not specified in the regulation; they are rather described as an ability that is made possible by the situational awareness achieved by the ESP. According to the regulation, "reaction capability" means "the ability to perform actions aimed at countering illegal cross-border activities at, along or in the proximity of, the external borders, including the means and timelines to react adequately"[53]. This definition does not provide a qualitative benchmark of reaction capability either in terms of a defined timeliness of the reaction or in terms of objectives. It also does not refer to any legal basis for interventions, or mention that this definition addresses law enforcement units, whose reaction capability is a concern. Rather, it stresses that the "ability to perform actions" and "the means and timeliness to react adequately" result from the quality of the ESP. What is unsettling here is the fact that the humanitarian intention "to be better able to reduce loss of lives of migrants" is included in the "situational awareness," but is not mentioned as one of the results of this awareness. Saving lives is not part of its defined reaction capability.

51 EUROSUR Regulation (EU) No 1052/2013, Art. 3(d).

52 Ibid, Art. 3(b).

53 Ibid, Art. 3(c).

Overall, the generation of the object of knowledge itself, the ESP, is underlined as the means and ends of the exchange of information in the EUROSUR network. The argument, or evidence, for taking reaction measures is visually presented on the electronic map of the ESP. However, it is visualized "on the basis of combining new information,"[54] such as operational information or signals, and fused with "existing knowledge,"[55] such as available data or databases. According to the Head of Research and Development at Frontex, the ability to electronically leave their national border and see (and compare) what is happening at other parts of the external borders not only supports solidarity among authorities – in the sense that, for instance, Polish authorities *see* that the Italians have much to do – it also allows them "to understand parallels."[56] He explains:

"Normally, the member state, they should know what they are doing at their external borders […] in that sense it isn't additional information, they know where the patrol units are, so in that sense it is nothing new. However, they can see that at the border between Ukraine and Slovakia that a new modus operandi is popping up there and, I don't know, Chinese are appearing there at the border with false documents, so they might think: 'Okay if we see Chinese at our border we might want to check a little bit further and verify whether these documents are really the correct ones.' And this tool to understand parallels is not available in Europe at the moment."[57]

However, matching data and conducting a risk analysis – factors alluded to in the definition of situational awareness – go beyond profiting from the experiences of other authorities and border guard colleagues. Moreover, they also go beyond the mere purpose of information exchange. These computerized analyses rather produce knowledge and generate scenarios. They project models of how and where the border will probably (or possibly) be subject to pressure in the future. In this attempt to understand parallels, the "emphasis is on what can be conducted 'across' items of data, on and through their very relation" (Amoore 2011: 30). However, this relation is a data correlation, and it serves to detect anomalies in a set of data. As such, it operates in a self-referential manner. The (future) risks emerge according to how the filters have been defined.

54 EUROSUR Regulation (EU) No 1052/2013, Art. 3(b).

55 Ibid.

56 Head of Research and Development at Frontex, personal interview (May 27, 2011).

57 Ibid.

Since the prognostic criteria and indices for data analyses are defined by the agency itself, the European situational picture is critically influenced by Frontex's services and risk analysis. In fact, a careful reading of the composition of the ESP as defined in Article 10 of the EUROSUR Regulation reveals that the ESP is, in fact, abounding with Frontex's risk analysis and processed information. Inti Schubert's observation that the generation of situational pictures enables authorities (here Europol) "to define the requirements for their intervention themselves" (Schubert 2008: 177) proves true in the case of the ESP. Although merely a coordinator, the Frontex agency is in the position to produce a dynamically developing knowledge base that serves to justify and legitimize border control, surveillance and intervention measures.

4.3 THE COMMON PRE-FRONTIER INTELLIGENCE PICTURE (CPIP)

The common pre-frontier intelligence picture (CPIP) was planned as a "service to the EUROSUR."[58] Its service consists in the contribution of information to the European situational picture (ESP). Although the CPIP was launched separate from the EUROSUR IT application, its content is ultimately visualized together with the ESP: "technically, the ESP and the CPIP are one."[59] In practice, this means that the information collected for the CPIP appears together with the ESP on the same screen in the same map. Contrary to its technical fusion and visual indistinguishability, however, the regulation lists the CPIP as a separate situational picture that is different from the ESP and the national situational pictures.[60] Moreover, its information is described as being from the "pre-frontier" and as leading to an "intelligence picture." We must therefore ask, if the differences do not appear onscreen, what kind of situational picture is this? What sort of information is this about? And where is the pre-frontier area?

Research and development for a common pre-frontier intelligence picture (CPIP) was conducted by a German company called Electronic Systems GmbH (ESG) together with the University of the German Federal Army Munich as a subcontractor, with cooperation from the subcontractor EADS. Drawing up a

58 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

59 Formulation used by an EC official in December 2012.

60 EUROSUR Regulation (EU) No 1052/2013, Art. 8.

CPIP concept was one of the sub-projects of a larger contract with ESG for the EUROSUR technical study.[61] The task of the CPIP subproject consisted in proposing a way to provide member states with a comprehensive information base, while at the same time leaving their authority over information untouched. The study's final report, presented to the Commission in January 2010, provides insight into the sources and the kind of "intelligence" considered usable for the CPIP.[62]

In the report, the CPIP is intended to "provide the national coordination centres (NCCs) with effective, accurate and timely intelligence […] in a frequent, reliable, interoperable and cost-efficient manner,"[63] In terms of the CPIP concept, not only the quality of the data is intended to matter, but also the quality of the service of providing information in and of itself. In fact, this service served two purposes: a) member states were to receive information that would be "out of scope" for them to collect, access or produce themselves; b) in addition, they were to receive new information frequently, cost-free and via reliable and interoperable channels. The advertisement directed at member states is clear: CPIP offers you more information, processed according to your interests, without extra cost or effort. The distinction between "items that are *in scope* of the CPIP and those that are *out of scope*,"[64] which the report lists in tabular form, deserves a closer look. *Out of scope* for the CPIP is any information collected within the

61 In January 2009, the Commission contracted Electronic Systems GmbH (ESG) to do a "Technical study on developing concepts for border surveillance infrastructure, a secure communication network and a pre-frontier intelligence picture within the framework of the European Border Surveillance System" referred to as the EUROSUR technical study [hereafter cited as EUROSUR technical study]. The study is divided into three subprojects: namely, the management concept (subproject 1), the communication information system (CIS) (subproject 2), and the common pre-frontier intelligence picture (CPIP) (subproject 3).

62 The study is designated intellectual property of the Commission, which is why approval from the Commission is required for each citation. Inquiries made directly to the ESG are also referred back to the Commission. In a conversation on the phone with a representative of the ESG, my identity as a PhD student of sociology was questioned and I was asked if I were not rather from a "leftist newspaper." All quotations cited in this work have been authorized by a spokesperson of the Commission during a personal conversion in 2016 with the concrete citations at hand.

63 EUROSUR technical study, subproject 3, p. 11.

64 EUROSUR technical study, subproject 3, p. 19, original emphasis.

sovereign territory of the member states or Schengen associated countries. For the purpose of the CPIP, no information or intelligence can be collected from within a national territory. Furthermore, information that is relevant for defense, personal data and law enforcement activities other than border control are out of scope for the CPIP.[65] Essentially, this distinction keeps the supranational level of the EU out of member states' bureaucracies. The proposed CPIP does not interfere with national administrations, security procedures or other sovereign competences. Conversely, the report envisions the "geographical area beyond the territory/external border of EU Member States and Schengen associated countries […] with main focus on neighbouring third countries" as being "in scope" of the CPIP, thus circumscribing this area as pre-frontier. The CPIP is also designed to include information on "border management in third countries" as well as information that is processed, that is, analysed or matched, against other databases.[66] Furthermore, there is information submitted from many possible sources, like embassies, to official informants, like the immigration liaison officer (ILO), as well as types of information, like open-source intelligence (OSINT), imagery intelligence (IMINT) and signals intelligence (SIGINT). The CPIP sub-report offers a compilation of information and information channels that it would be "nice to have."

Since most of these sources found their way into the draft regulation, Hayes and Vermeulen expressed the concern "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" (Hayes/Vermeulen 2012: 20). Despite seemingly limitless ambitions and ideas for synergy, the actual CPIP service still was described as "a very rudimental collecting system"[67] during the development phase. According to the EUROSUR project manager at Frontex, "the purpose of EUROSUR is to make this more, let's say, routine, and assign someone responsible, which is Frontex."[68] In the end, Frontex's Risk Analysis Unit (RAU) was tasked with establishing and maintaining the CPIP. It can be assumed that the task of composing the CPIP was not taken lightly by the Risk Analysis Unit, as it had to adapt to the expectation of a 24/7 service and thus the notion of an early warning system, while risk analysis at Frontex had actually thus far been con-

65 EUROSUR technical study, subproject 3, p. 19.

66 Ibid.

67 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

68 Ibid.

cerned with long term studies, annual or quarterly reports and the formulation of risk indicators, etc.

Ultimately, the CPIP was not drafted as a separate informational layer or separate electronic map, like the national situational pictures, but as a draft of a sphere of supranational competences in border management that evolves *qua* informational affiliations and access. As a result, national territories and informational sovereignty are explicitly out of scope, while everything else that may affect the EU external border could be in scope of the CPIP. In order to concretize supranational interiority as a sovereign place for the postnational EU external border, the CPIP has been developed along the notion of the information exploitation and coverage of the pre-frontier area.

4.3.1 The Pre-Frontier: Risks, Surveillance and the Elsewhere

When asked about the specific nature of the CPIP, a Frontex official stated that it was "just exchanging information which is not coming from the border but before the border."[69] In a similar vein, the EUROSUR Regulation defines the pre-frontier area *prima facie* in geographical terms. Yet, it is also completely boundless as "the geographical area beyond the external borders,"[70] In other words, the pre-frontier is non-EU, it is the rest of the world whenever it affects the external borders of the EU. With regard to the CPIP, "border–related" does not result from having a geographical proximity to the political and administrative borders of individual member states, but from being passed through an informational filter. The pre-frontier is an "amorphous domain" (Pugliese 2014: 578) characterized *ex negativo* as not interfering with national sovereignty. Likewise, the draft regulation proposed that pre-frontier may be defined as "the geographical area beyond the external border of Member States *which is not covered by a national border surveillance system.*"[71] This statement illustrates the added value of CPIP for the member states, because it contributes information that cannot be generated with the authority and the border surveillance systems of the individual member states. The added information can be interpreted as *the* critical incentive for the member states to participate in EUROSUR and to engage in exchanging information themselves. However, as we have seen with other incentives of the development phase, the incentive has become invisible in the final regulation

69 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

70 EUROSUR Regulation (EU) No 1052/2013, Art. 3 (g).

71 EUROSUR legislative proposal, COM(2011) 873 final, Art. 3 (f), emphasis added.

proposal. The pre-frontier is thus blithely defined as "the geographical area beyond the external borders."[72] Instead of a geographical place (not even of the extra-territorial kind), it is rather a network of cooperation, sources and references.

Furthermore, the notion of pre-frontier encompasses the notion of a dark field, of the unknown and of futurity. This dark field needs to be explored, illuminated, explained and put on the screen. In the indeterminability (and liminality) of the dark field, the assessment of risks and the sovereign mandate to restrict people's liberties merge easily, because the potential deviances in the dark field seem to call for action (Denninger 2008: 94-95; Aradau/Lobo-Guerrero/van Munster 2008; Ellebrecht 2014b). When relating strategic measures to risks, this brings about the "paradoxical situation that action must be taken although there is ultimately no basis for the action" (Nassehi 1997: 169-171). Pugliese describes the empowering modeling of possible risks as the "multi-layered aspect of the 'pre' – pre-frontier, pre-emptive risk, precautionary assessments and so on" (Pugliese 2014: 579). This intimate relation between pre-emption, virtual suspicion and scanning data for risks is also illustrated in the description of CPIP information.

S.E.: If you look at the different outlines and comments on the EUROSUR, then the CPIP seems to be the big thing.

P.M.: Sabrina, I told you, that you only collect information if you are going to act. If you are not going to act, why are you collecting information? So, CPIP should be a source of information that allows you to be proactive and not reactive, so that you know what is coming to you. For instance, you know that there is a group of people which are gathering in Georgia and they are planning all of them to cross to Europe, and to all, in block, require asylum – that is information that would be coming from the pre-frontier area. […] Or you know that there is this ship which is known to have been involved in traffic of tobacco before, that is now leaving Odessa, and then the Rumanians and Bulgarians are together and say: "Okay let's see where this guy is going this time." This is CPIP. […] Look, one of the sources is OSINT, open source, so you have information of traffic of ships and traffic of merchants, which is very much accessible. But if you are able to analyze this information you may find anomalies, in the container traffic for instance. Anecdotally, there is a JRC, joint research center project, which is analyzing the moving of 8 million containers and telling the member states: "We have identified this which seems to be doing something strange." And the hit of the cases in which they were right is about 50

72 EUROSUR Regulation (EU) No 1052/2013, Art. 3 (g).

per cent. When they say this container is suspect, 50 per cent of the time there is something strange. This is CPIP.[73]

The situational picture of the pre-frontier presents information "that allows you to be proactive," but instead of working with legal evidence, it works with a virtual suspicion. Policing based on collected knowledge and experience is not new ("let's see where this guy is going this time"). What is new is that this knowledge comes from a database and has been evaluated through algorithms and is no longer tied to the experience of the border guard doing the assessment. In information-based border management, a suspicion no longer develops through a concrete operational situation on a border, but within the national coordination centers and analytical institutes, in particular the Frontex Risk Analysis Unit (RAU). The "seeing like a border" called for by Chris Rumford (see for instance Rumford/Geiger 2014) is also embraced and managed by Frontex, although not cosmopolitan in outlook. The gaze on the border reality rather is "more technologically and statistically mediated and 'datafied'" (Broeders/ Dijstelbloem 2016: 242). Judging by the premise of "if you are able to analyze the information" stated in the interview, the interest in and use for data and information is potentially unlimited.

The EUROSUR Regulation allows for the electronic monitoring of the pre-frontier area and therefore transfers the coordination of "the common application of surveillance tools"[74] to Frontex. The agency is thus again awarded a strong power over knowledge because it can define, or rather select, the targets to be monitored and the kind of data to be collected and processed. The task of supplying "national coordination centres *and itself* with surveillance information on the external borders and on the pre-frontier on a regular, reliable and cost-efficient basis"[75] distinctly goes beyond the act of providing a service. Rather, because Frontex is a coordinator, it is also a management tool and an authority.

Frontex can generate surveillance information through a variety of different information sources and surveillance apparatuses. First, the agency can monitor selected harbors in non-member states via satellite image.[76] Through these satellite images, Frontex can monitor the coastlines of non-member parties in order to determine potential landing sites for small boats that can be used for refugees

73 EUROSUR Project Manager at Frontex, personal interview (May 15, 2012).

74 EUROSUR Regulation (EU) No 1052/2013, Art. 12.

75 Ibid, Art. 12 (1), emphasis added.

76 EUROSUR Regulation (EU) No 1052/2013, Art. 12 (2a), (3b).

and migrants. Second, the agency can also evaluate shipping traffic information.[77] The evaluation of various tracking signals[78] allows them to locate vessels that are not sending signals and therefore cannot be identified. Because the monitoring and tracking of shipping traffic occurs via a comparison of signals that have already been received, all vessels that do not send signals are suspected. As a result, the line separating not-identified and potentially dangerously become fluid (Mallia 2010: 34). In addition, the suspicious lack of signals of certain boats and the SOS calls of vessels in distress are also relevant pieces of information when creating an overall picture. When visualized and integrated into discussions, this information creates opportunities for border guards to intervene (Miltner 2006: 84-85). Third, additional selected maritime areas or parts of the pre-frontier area can be monitored.[79] with "sensors mounted on any vehicle, vessel or other craft."[80] Frontex decides which areas, harbors or vessels to monitor based on its own risk analysis. Although its declared aim is to provide member states with information, it also admits that the "agency may use on its own initiative the surveillance tools referred to in paragraph 2 for collecting information which is relevant for the common pre-frontier intelligence picture,"[81] Finally, the visualization of border-related incidents in the pre-frontier area, regardless of how this occurs, – whether as dots, satellite imagery or incident reports – normalizes its somewhat extra-territorial mandate by suggesting a transformed topography of operational borders. The legal borders of policing thus become more mobile as the CPIP becomes more routine.

The self-reflexive reference to CPIP amplifies Frontex's competences. As an official of the European Parliament in Brussels said while shaking his head during the negotiations for the EUROSUR Regulation, "CPIP is Frontex," Indeed, assigned with the task of establishing the CPIP and ESP, Frontex has become not only an institutional hub through which information concerning the pre-frontier area can be collected and made graphically understandable; it has also become a

77 EUROSUR Regulation (EU) No 1052/2013, Art. 12 (3a).

78 Ships are to report their identity and position four times a day to Long Range Identification and Tracking System (LRIT) data centers. The implementation of LRIT is mandatory for all ships with over 300 gross tonnage as of May 2006. Information from the Vessel Monitoring System (VMS) or the Automatic Identification System (AIS) can be used without a ship's consent (Mallia 2010: 34-37).

79 EUROSUR Regulation (EU) No 1052/2013: Art. 12 (2e).

80 Ibid, Art. 12 (3c).

81 Ibid, Art. 12 (5).

service provider that has and distributes statistical information about crossings of the EU's outer borders. Thanks to EUROSUR, Frontex is no longer merely an agency acting as a neutral coordinator on behalf of a supranational state; it is rather a "centre of calculation" (cf. Latour 2003: 215-257) for its border.[82]

At the same time, the CPIP is not an information layer or a separate electronic map, like the national situational pictures, but a description of competences. CPIP is the supranational sphere of competences, agreements and access. Regarding the ESP, it lets risk analysis and operational recommendations be integrated into the way national authorities see and interpret situations along the external border of the EU. To Frontex, the CPIP is an instrument for bridging the gap between management and mandate.

4.4 EUROSUR ON THE SCREEN: THE DEPICTION OF AN EXTERNAL EU BORDER?

As Gordon Fyfe and John Law point out, a "depiction is never just an illustration. It is the material representation, the apparently stabilized product of a process of work" (Fyfe/Law 1988: 1). In this section, I began by unfolding the process of work that was necessary for developing a network that facilitates the exchange of information and analysis between border authorities in the EU. I then outlined the visualization and integration of this data on the screen as a European situational picture (ESP) and a common pre-frontier intelligence picture (CPIP) respectively, and I discussed the premises and arguments of the electronic depiction. Effectively, the EUROSUR IT network is as much a result of a process of work as it is an ongoing process of constant work on the ESP. I thus analyzed the EUROSUR on the screen as both a result and a process.

In tracing the development of the network, it quickly became clear that the challenge presented by this process of work did not consist in the technical details of the GIS's configuration, programming or software design, but rather in the acceptance of and compliance to the system by member state authorities. Still, the flexible and non-committal method used to test the IT application strongly contributed to convincing member states to consider the system in the

82 I used this characterization already in an earlier publication (Ellebrecht 2014b: 180). It has also been advanced by Dennis Broeders and Huub Dijstelbloem (2016: 243) in an essay publication.

first place and gradually led to an increase in trust and compliance among participants. The communication format and the rules of information exchange between member state authorities were geared toward the usability of the graphic user interface.

Indeed, an issue of sovereign competences was translated into an issue of software design and was solved as such. Correspondingly, different national angles were arranged in the GUI under menu items, domains of competence were translated into GIS layers, and different political hierarchies were flattened to nodes in the system. Ultimately, it was probably easier to get used to menu items for the purpose of testing an IT application than to agree on common priorities for border policies in Europe.

However, the EUROSUR on the screen did more than just allow the reconstruction of the process of work that went into it. The electronic map of the ESP, the "EUROSUR on the screen," not only provides an image to the added value of information exchange and not only demonstrates that all the extra work and the institutional reconfigurations are worth it, it also offers what Latour has called a "new visual language" (Latour 1986: 19) that allows the external border of the EU to be 'seen' as a supranational entity.

Indeed, it is not border guards and Frontex officials who now have the new supranational border in mind and in plain view – a supranational EU external border is not a thing that border guards or foreign ministers all of a sudden see and thereof take for granted. It is not a new thing that can be seen from one moment to the next, from the moment of signing the Schengen Agreement or its Europeanization in the Treaty of Amsterdam. It is rather the case that "the same old eyes and old minds" are now applied to the communicational format of the EUROSUR network, which allows them to naturally see the external border of the EU as a job description. The EUROSUR on the screen offers the "new fact sheets inside new institutions" (Latour 1986: 15), which allows the old heads to naturally see the common border. Incident reports and impact levels are distinct features of this new fact sheet. As boundary objects (Star/Griesemer 1989), they unite national issues at the border with ambitions of European border management. Hence, the "EUROSUR on the screen" can duly be described as a "giant 'optical device' that creates a new laboratory, a new type of vision and a new phenomenon to look at" (Latour 1986: 19).

In many ways, the EUROSUR items differ from the cartographic depiction of political borders and the treaties on them in the modern frame. First and foremost, EUROSUR's electronic map provides a situational picture and not a representational map. The electronic map displaying the European situational picture

is the tangible result of both the exchange of information and institutional reconfigurations in EU border policies. It is the epitome of the system and the focal point of the regulation. The regulation, in turn, defines how situational pictures are to be produced, namely "through the collection, evaluation, collation, analysis, interpretation, generation, visualization and dissemination of information." In fact, the European situational picture is based on a reversed relationship between the notion of border and the notion of selection: the drawing of a line as a benchmark to selection has given way to the drawing together of disaggregated sources and information which visually cumulate by their geo-code; homogenous territory on the one side, constantly changing distribution and assessment of risks on the other. In this sense, Rocco Bellanova and Denis Duez aptly describe EUROSUR as a "continuous effort of mise-en-discourse" rather than "an addendum or technical fix" (2016b: 40).

This chapter has shown that EUROSUR brings about the laboratory, the vision, and ultimately the "new phenomenon to look at" (ibid). While the different NCCs and Frontex RAU are networked as the "new laboratory" producing knowledge and maps of border-related incidents, the ESP embodies the "new type of vision." This vision assembles on the screen, where it benefits from "the appearance of a neutral and depoliticized form of calculation" (Amoore 2009: 20), even though it integrates discontinuously generated data and the most diverse ways of obtaining information and suspicion. Ultimately, the ESP provides a view of the situation at the external borders and a vision of cooperation, joint tasks, and operational urgencies. The exchange of information thus produces a picture, a vision, and affords a supranational mandate to react.