SOURCE | Societal Security Network

VIRTUAL CENTRE OF EXCELLENCE FOR RESEARCH SUPPORT AND COORDINATION ON SOCIETAL SECURITY

D2.3 SECTOR SURVEY MEETINGS AND REPORT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 313288.

D2.3 Sector survey meetings and report

Abstract: This report is a summary of the sector survey meeting that was organised by the SOURCE Network on the 5th of June 2014 in Brussels. During the meeting, representatives from different professions and institutions and the partners of the SOURCE consortium discussed a number of security problems and solutions, following a structured approach of decision support for security solutions, based on the DESSI method.

Contractual delivery date: 31 July 2014 (M7)

Actual delivery date: 11 August 2014 (M8)

Version: 1

Total Number of pages: 32

Authors: Reinhard Kreissl, Alexander Neumann, Meropi Tzanetakis (IRKS)

Contributors: PRIO, CIES, Fraunhofer INT, TNO, EOS, Tecnalia

Reviewers: Fraunhofer INT, PRIO

Dissemination level: PU

Deliverable submitted 11th of August 2014(M8) in fulfilment of requirements of the FP7 project, SOURCE – Virtual Centre of excellence for research support and coordination on societal security (SEC-2012.7.4-2: Networking of researchers for a high level multi-organisational and cross-border collaboration)

Contents

Introduction

This report is based on the sector survey meeting organised by the SOURCE network on the 5th of June 2014 in Brussels. The SOURCE network identified five different sectors of security actors that are highly relevant for the further development and establishment of the SOURCE network. Further members of the network should be recruited from the following 5 sectors:

1. social and human science researcher communities
2. security industry actors (incl. technology developers)
3. End-user
4. security policy-makers
5. civil society actors

About 20 invited representatives from different professions and institutions, including partners of the SOURCE consortium discussed a number of security problems and solutions, following a structured approach of decision support for security solutions, based on the DESSI[1] method (see chapter 2). Working on two scenarios (security in public transport and migration into the EU across the Mediterranean Sea) industry representatives, researchers, policy makers, civil society representatives and End-users analysed a number of options, bringing their sector-specific expertise into the discussion.

The chosen format of this meeting produced lively discussions and demonstrated how mutual learning effects can be achieved when bringing together representatives from different fields and backgrounds. The cognitive and normative limitations, shaped by different professional and institutional affiliations became clearly visible and mutually understandable, clearly demonstrating that decisions about solutions for security problems require a multi-professional and inter-institutional discourse.

This report (D2.3) is a summary of the meeting held in Brussels. In the next step, the SOURCE network will use this report as the basis for interpretation and analysis of modes of exchange between the relevant sector representatives (D2.4) to further build the network.

[1] http://securitydecisions.org/

1. Scenario approach – The DESSI Method

For the D2.3 sector survey meeting task leader IRKS decided, in consultation with the other partners of the SOURCE network, to provide a framework for the workshop that enables the SOURCE network on the one hand to gather data about different security claims raised by the invited experts and on the other hand to allow the guests of the network to obtain new practical knowledge. All representatives from the five sectors share a common interest: they all address **security problems** in their daily work. Thus, we decided to develop a problem-centred scenario approach that allows the representatives to refer back to their practical knowledge about solving security problems. The scenario based quasi-experimental design of the T2.3 Sector Survey Meeting had two objectives: It should offer invited security experts an opportunity to learn a new method for assessing and solving security problems and it should enable the SOURCE network team to observe and explore "modes of interactions" (relevant for T2.3) and the "security claims" (relevant for the analysis in T2.4). The SOURCE network decided to use the DESSI method. DESSI is a structured approach to address security problems and **involve several perspectives** in the discussion. DESSI was developed in an FP7 research project led by the Danish Board of Technology.

DESSI – Decision support on security investments:

"DESSI is a method for decision support that takes the complex dimensions and dynamics of modern society into account. By assessing a security solution's impact on several important societal dimensions, DESSI assists in making decisions for a well-grounded and robust investment. Bringing together knowledge from a broad field of experts and methods, DESSI will help to make better security decisions."[2]

The **DESSI method** engages policy makers, decision makers, End-users, experts from industry and civil society actors in a **participatory decision making process**. For the purpose of the SOURCE sector survey meeting the SOURCE network slightly modified the DESSI approach to generate a problem-oriented scenario approach.

The DESSI process is divided into three phases:

1) Security Problem Description	
Used in **DESSI**	Used in the **SOURCE** T2.3 sector survey meeting
The aim of the first phase of DESSI is to describe the security problem or challenge as detailed as possible. This first step should help the "problem owner" to develop a broader understanding of the problem. The security problem description is going to be used throughout the next two steps in the DESSI process and therefore should carefully identify the groups who are affected by the security problem and provide an overview of the needs that are going to be satisfied by the potential solution(s).	In SOURCE we used the "Security Problem Description" as the "security scenario" that we wanted to discuss with the invited experts from the five SOURCE sectors. The "security scenario" was used as a frame of reference for discussion. Furthermore the "security scenario" was adapted according to the background of the invited experts. E.g. we discussed a "public transport security scenario" with public transport experts.

[2] For more Information on DESSI see www.securitydecsions.org

2) Security Investment and alternatives	
Used in **DESSI**	Used in the **SOURCE** T2.3 sector survey meeting
During the second phase of DESSI the possible solution to the problem described in phase 1 shall be identified. In the DESSI process this phase would require a workshop where the DESSI moderators guide the workshop participants through this step and try to develop and discuss as many alternative solutions as possible – until they arrive at the most relevant solutions, which then are going to be assessed in the third and final stage of the process.	In SOURCE the potential solution was part of the "security scenario" that was used as a frame of reference for our workshop with the sector representatives.

3) Multi-Criteria Assessment	
Used in **DESSI**	Used in the **SOURCE** T2.3 sector survey meeting
In the final workshop of DESSI the participants are divided into groups and they will address different solutions to the security problem along the dimensions of DESSI for assessing security problems and solutions. Key for a successful DESSI process is the involvement of external experts. The expertise of those external experts should cover technological, legal, societal, economic and cultural aspects of the solutions that are going to be assessed in the final DESSI workshop. For the final assessment workshop DESSI is using a set of 42 predefined questions that should trigger a discussion about the usability, usefulness and the relevance of the proposed solutions. Those 42 questions can be edited in the DESSI web tool which is the main supporting tool for the DESSI moderators to structure the workshop.	Partners IRKS and Fraunhofer INT adjusted and reduced the total number of the original DESSI questions for our purposes in SOURCE. Whilst in DESSI the answers to those assessment questions provide a ranking of the potential solutions tested in the process, **in SOURCE we used those questions to trigger a discussion amongst the invited sector representatives**. The questions that had been reviewed and reformulated by IRKS and Fraunhofer INT helped us to operationalise the security claims that are of interest for the analyses of the workshop results in the upcoming Task 2.4 which is based on this report.

DESSI DIMENSIONS FOR ASSESSING SECURITY PROBLEMS	T2.4 SOURCE SECURITY CLAIMS
1) Security gain or loss (PRIO, EOS)	Security values
2) Fundamental rights and ethics (IRKS)	Morals
3) Legal Framework (KCL)	Cultural ideals
4) Social implications (KCL)	Cultural ideals
5) Acceptability (TNO)	Social norms
6) Political significance (FHG)	Political riorities
7) Economy (FHG)	**New Claim:** Economics

To trigger a discussion about security claims and to observe modes of interaction between the representatives from the five different sector two security scenarios were presented to the participants. After the presentation of the security scenario the discussion began and was guided by the DESSI questions that had been reformulated by IRKS and Fraunhofer (see chapter 3). The two scenarios (1: security in public transport and 2: EU border control) were chosen along the field of

expertise of the invited sector survey representatives. The idea behind that was to enable the sector survey representatives to argue during the discussion that was triggered by the DESSI method on the basis of their actual work experiences in their day to day work with security problems.

1.1. Scenario 1: Security in Public Transport

Aim: To prevent further attacks on the bus drivers

The Austrian public transportation organisation 'Austria Transport East (ATE)' operates around 80 per cent of the bus market in Vienna and 60 per cent of the overall Austrian bus market. ATE is also operating the Viennese underground system and the rapid transit railway in eastern parts of the country (greater Vienna area). Per day 3.5 Million passengers are using the ATE services in Vienna and its surrounding areas.

Over the last 6 months ATE's bus drivers had been confronted with the following security problem: During the night shifts (after 10 p.m.) individuals or groups were physically attacking or verbally harassing ATE's bus drivers. Moreover, the rise of cashless methods of payment has made busses targets for robberies, despite the cash holdings being relatively minor sums. According to recent police investigations the various incidents were not interrelated. In the last couple of weeks three Viennese bus drivers had been physically attacked during their night shift. This resulted in a 12 hours lasting general strike involving all bus lines in the whole ATE operating area. The trade union and the staff council were demanding the implementation of a video surveillance system (CCTV) in all Viennese buses to protect drivers. In Vienna ATE is operating around 500 buses, in about half of them CCTV is already installed. Available evidence suggests that CCTV does not affect the number of incidents registered. Passengers become very rarely victims of attacks in public buses. ATE's executive board has commissioned a group of experts to assess the following investment options to solve the security problem.

Investment 1: Protected transparent box, aka shield

Since the first incidents happened half a year ago ATE started to invest into protected transparent boxes. These "shields" are very common in England and the Netherlands but for Austrian standards this is a new measure, as bus drivers are seen as respected figures with strong authority on his own who wouldn't need to be protected by a "glass shield". Responses from ATE's bus drivers regarding the "shield" were mixed. Some appreciated this measure and reported to the employee organisation that they now feel more secure. Others didn't like the measure at all as they felt somehow "isolated" from passengers.

Investment 2: CCTV (record only) in all buses

The second investment (alternative 1) - video surveillance in all buses - was favoured by the staff council and the trade union. A CCTV camera should be located near the bus driver's seat to have video footage of perpetrators available in case of incidents. The camera is permanently recording the front entrance of the bus and the area behind the drivers. Footage is stored for 72 hours and then deleted if police or ATE is not requesting it. The camera would not monitor other areas of the passengers' compartment, although it is unclear how much behind the "back of the bus driver" will be monitored. Another reason why this measure is so popular is that two major tabloids available for free at all bus and metro stations in Vienna were campaigning for more security for passengers in buses through video surveillance although attacks on passengers have not significantly risen in the past 12 months.

Investment 3: Conflict management, communication and stress relief

ATE understands due to recent incidents that their employees, especially the bus drivers in Vienna, are highly concerned about their personal safety and therefore is considering implementing several "soft measures" to reduce the pressure on their employees. These "soft measures" will include trainings and seminars on conflict resolution, trainings in communication strategies and the option of supervision/counselling with a psychologist in case of an incident. All these measures aim to increase the perceived security amongst bus drivers.

1.2. Scenario 2: EU Border Control

Aim: assess possible security measures (and alternatives) dealing with the following specific security problem with the DESSI methodology.

The Mediterranean area is a target region for immigrants from African countries entering the EU. Lampedusa, an idyllic Italian island in the Mediterranean Sea, is confronted with high numbers of boat arrivals each year. Lampedusa is perhaps best known as an entry point for migrants hoping to make their way to the European mainland. Geographically closer to North Africa than Italy, the island is a gateway for migrants from Africa, the Middle East, and Asia. Many refugees are applying for asylum as soon as they reach EU territory. For reaching their destination, many risks are accepted by the immigrants. This includes the willingness to risk their lives and become indebted to traffickers/smugglers.

Frontex has already taken some security measures, such as dispatching ships, planes or helicopters to patrol coastlines. However, these measures are insufficient in preventing and tackling the ongoing "problem" of migration. Therefore, two possible security measures are offered:

Investment 1: An Autonomous Marine Surveillance System (AMASS[3]) – 24/7 surveillance, 360-degree view of the area above water, fully functional in all weather conditions

AMASS comprises a network of unmanned platforms located a considerable distance from shore. Each platform is fitted with cutting-edge sensors and operates self-sufficiently, i.e. without the need for manual intervention. Visual and acoustic data captured by the sensors is transmitted to a central command centre. If suspicious small and midsize vessels are detected, a crew can be dispatched to further investigate the situation or take any other action.

This provides authorities with early warning of il/legal activities at sea and enables them to take appropriate action to improve overall protection of European shores. AMASS is being developed by a FP7 project of the same name led by Carl Zeiss Optronics. AMASS is aiming at a pioneering yet proven solution – leading to safer, more secure coastlines.

Investment 2: Refugee advisory centre in Tunisia

10,000 refugees have drowned while attempting to reach Europe in recent years, according to estimates by the European Commission. Therefore, the alternative security measure aims to support the refugees on-site in Tunisia. The basic idea of such an advisory centre is to inform the immigrants that they have no chance of entering mainland Europe because they will be picked up by EU authorities before reaching EU territory. Additionally, refugees are going to risk their lives when trying to come into Europe. Instead, immigrants will be offered a legal option at the refugee advisory centre. The situation of every single immigrant will be evaluated and a procedure will be developed

[3] http://www.amass-project.eu/

to offer legal migration possibilities. The refugee advisory centre intends to reduce migratory pressure in the countries of origin.

2. Security claims and modes of interaction

The D2.3 report will serve as part of the data pool that is going to be analysed by Task 2.4. The security claims that have been identified are 1) security values, 2) political priorities, 3) social norms, 4) cultural ideals, 5) morals and 6) economics. The following documentation of the workshop is anonymised and is aiming to provide narratives for the further analysis of security claims. The comments from the discussants are sorted according to the five sectors the participants were representing. Since similar arguments were made in different contexts some statements will appear several times under different headings.

2.1. Security values

by PRIO and EOS

DESSI Tool Question	What is meant to be triggered with this question
Question 1): Will there be a measurable improvement of security?	Intends to find out which understandings of security the sector representatives have. *Will it help to preserve the status quo? Or, will it change the security situation in any measurable (objective) way? If so, then for whom and how?*

Sector 1: Social and human science researcher communities

Scenario 1:
Social researchers argued that cameras in scenario 1 would not deal with verbal aggression. All sector representatives agreed with that statement.

Researchers expressed their concern that in the presented scenario and in many real life examples a control system is mainly trust based, and to give trust to technology will reduce the feeling of security and damage the existing trust based system.

The **social researchers** agreed that the overprotection of the driver could become a new challenge. Young troublemakers could try to find another way to bother the driver.

Scenario 2:
A **researcher** mentioned that intelligence services actually know when boats are leaving, where they are and when they will arrive. This means that maritime automatic surveillance is of no use.

A **researcher** questioned who would be in charge of such a centre, the EU, UNHCR, local authorities? This would create a very complex situation. The authorities dealing with migration are part of hugely sophisticated networks, the centre would need to be highly organised to be able to give proper advice.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: In addition to the negative effects on the driver (isolation, potential health issue...), **industry representatives** were of the opinion that a shield or box could cause more troubles for the drivers as it can be attractive to throw things at it. It can even have a negative effect on protection, as it doesn't allow the driver to ask for respect as he is locked in a box. Also, if youngsters cause troubles (making fire, scratches, harassing passengers …), the driver will be forced out of the shield upon which he will be in danger anyway. The measure thus only delays the danger.
An **industry representative** shared his experience with regards to measures helping to improve security in buses: having visible cameras, shoulder height instead of under the roof, have a yellow sign showing that there is an active CCTV camera, a meter to measure visually the height of the attacker, have a strong light on the driver, wear a uniform, have clean buses etc. The representative also presented a more advanced solution were the cameras would be linked to a central where the staff would get notified by the push of a button from the driver that something is going on. The central will then assess the situation and intervene in a microphone directly to tell the wrongdoers to stop and that the police are under way. With this mechanism, cameras are more than surveillance as they allow acting directly. A **social researcher** reacted on the light idea saying that if the light had a positive effect it might perhaps be enough to start with this instead of going for the video surveillance package. Another **industry representative** reacted on this saying that a light in the face of the driver of a bus at night can be an issue as it hampers the view. The **industry representative** reacted by saying that aggression on bus drivers shouldn't be minimalized as the drivers are more and more stressed to go to work.

An **industry representative** suggested that less human surveillance and more technological one may reduce human costs. For example, while delegating a tickets sale job to a machine you can provide more personnel to the other needed activities. Installing video surveillance cameras in a bus can give the camera the responsibility to take care of what is happening in the back of the bus while allowing the driver to concentrate on the road. However, if cameras are meant to support, there is always a human being behind to take a decision.

Scenario 2:
Representatives agreed that maritime surveillance wouldn't be useful as it doesn't deal with the most important question: what is done once a boat is detected? An **industry representative** however argued that there is always a risk in a large movement of people – "do we know who they are and what they intend to do?" Governments have to be conscious and careful about that. The representative used a metaphor asking people if they would accept that people enter their house without knowing who they are. (There was a lot of noise in the room because of the person bringing in the coffee so no one really picked this question up.)

An **industry representative** counter-argued that in the case the people wouldn't receive the right advice they would just go on the other way with smugglers who are very well organised – and "the real enemy in all of this". The representative added that people are taking massive risks but don't trust governments to advise them, which is why centres wouldn't work in this case.

Sector 3: End-user

Scenario 1: The **End-users** expressed scepticism to the argument brought forward by the **Social Scientist** that the efficiency of a measure has to be evaluated before judging if a measure was either successfully or not implemented. As they shared their impressions from their daily routines there is 'simply not enough time and money' to evaluate measures thoroughly with a scientific side study. Of

course every organisation will develop its own bench-mark criteria if a (surveillance or security) measure is working successfully but again, once the decision was made for one product/service the organisation will have to stick to that decision for a while.

End-users finally mentioned that that it was not possible to measure its efficiency.

Sector 4: Security policy-makers

Scenario 2:
A **policy maker** thought that a centre could at least divert the advices usually made by criminals to the people working in the centre.

Sector 5: Civil society actors

Scenario 1: **Civil society** was strongly concerned about the increase of the use of technology and said that taking responsibility away from an individual and giving it to technology removes societal engagement and reduces human experience. It is not possible to acquire the ability to manage risk if technologies offer all the solutions and take away your experience.

Civil society actors also mentioned that a shield would not protect against verbal provocation.

A **civil society** representative found that this totalised version of security was extreme for problems with youth causing troubles on buses.

DESSI Tool Question	What is meant to be triggered with this question
Question 2) Will people feel more secure?	Who are the people for each sector representative? *Will the felt security be the same for different societal groups - is it evenly distributed? For example, a security checkpoint can make some people feel secure and increase the anxiety for others.*

Sector 1: Social and human science researcher communities

Scenario 1: **Social researchers** mentioned that once there is a camera people delegate the responsibility to someone else. In the absence of a camera a passenger might feel he should help the driver but with a camera it is not his responsibility anymore.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1:
Industry representatives mentioned that even in the occasion where a shield would protect the driver the passengers could still be attacked, either because the driver is unattainable or because the driver is not necessarily the target. Industry representatives also agreed with the statement of the **policy makers** that passengers will feel less comfortable if they have less contact with the driver. They will receive a signal that it is not safe (since the driver is in a box), but the passengers are on their own.

Industry representatives also mentioned a case of a city where 15 years ago the drivers didn't want to drive with surveillance. However, now it is the opposite as it is in their contract that they will not drive if there is no surveillance. There has thus been a total shift in this case from being opposed to now demanding it – for security purposes. It therefore seems that in that case drivers feel more secure when CCTV cameras are present.

Other **industry representatives** mentioned that video surveillance could create another insecurity regarding privacy. People are afraid of being tracked and traced and are not being assured that technical solutions for protecting their privacy are in place. In order for them to feel secure they would need to be informed about the storing and protection of their data. This paradox means that passengers could feel safer with video surveillance – but would be afraid that someone traces all their data. Another **industry representative** argued that there is no evidence that people don't use buses because of surveillance. In a bus, passengers are trapped inside, unlike in the street where it is possible to run away from an incident. Cameras can bring comfort to people that if something happens it will be recorded.

Scenario 2: An **industry representative** mentioned that it was always important to distinguish objective real security and perceptive security. With transport issues it would be interesting to measure perceived security. Real security is measuring incidents; perceived security might also solve the problem. Both terms are getting mixed up because of the social scientist perspective, which is more about perceived security.

Sector 3: End-user

Scenario 1:
This question should help to figure out who is the subject of a security investment. For civil society actors, industry representatives, policy makers and the research community the answer was quite clear it is always about improving the situation of citizens. For the **End-users** it was different**.** Security for them is not only an issue that is addressed towards citizens (=people) in their understanding their colleagues and other field operatives (=people) are foremost the addressees of a security measure that should improve the (security) situation. For example in Scenario 1 **End-users** addressed the working environment of the drivers and the importance to encourage the drivers to report on the attacks.

Sector 4: Security policy-makers

Scenario 1: **Policy makers** believed that passengers will feel more secure if there are video surveillance cameras.

Sector 5: Civil society actors

DESSI Tool Question	What is meant to be triggered with this question
Question 3) Will the measure help to prevent future incidents?	What are the incidents the sector representatives are thinking about? Is it possible to determine the extent of preventive measures? Is the balance between prevention (lowering the risk to zero) and reaction (to an incident) important for the stakeholders? to which extent? Please explain.

Sector 1: Social and human science researcher communities

Scenario 1: **Research sector** supported the position that video surveillance would serve more a deterrence purpose than a detection one. **Social researchers** argued that conflict management was part of the general training on how to speak to passengers.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: **Industry representatives** mentioned that law enforcement forces and judges often couldn't use the tapes because of their poor quality. Another representative from the same sector argued that the quality is getting better and better and that was not a problem, the real concern being on what to do with it. The police will not be involved with verbal aggression for instance.

Sector 3: End-user

Scenario 1: **End-users** mentioned that an open climate for reporting any type of incident in all confidence is very helpful. It is therefore useful to train the users in conflict management, although this might be cultural (in some countries people might be reluctant to complain or report).

Sector 4: Security policy-makers

Sector 5: Civil society actors

Scenario 1: **Civil society** representatives saw little value in video surveillance as a preventive measure. As an example, video surveillance has been used in the UK for a long time however, the incidents still happen. Partly, they agreed that having screens on a bus projecting videos in real time may have a preventive effect.

DESSI Tool Question	What is meant to be triggered with this question
Question 4) Are decision makers free to take a rational decision on the measure?	When do you feel that a decision-making process is rational/efficient? *Sometimes an irrational overuse of security measures can be seen. Decision-makers may be driven by irrational demands from the public, the media, predefined policies or other drivers. This could for example lead to 'symbolic policies'. Free decision-making is seen as positive - whereas strong bindings are seen as negative.*

Sector 1: Social and human science researcher communities

Scenario 1: **Social researchers** argued that even though in some cases the drivers might be asking for surveillance this was not necessarily what the passengers wanted. They also pointed out that the cultural aspects need to be taken into account, some countries being more sensitive to surveillance than others.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: An **industry representative** argued that drivers feel it is not safe to work and use it an excuse to strike, "is as easy as that". Decision makers are therefore pushed to take measures.

Sector 3: End-user

Sector 4: Security policy-makers
Sector 5: Civil society actors

Scenario 1: **Civil society actors** mentioned that these types of measures are "attacking" an already marginalized portion of the society (in reference to the all-inclusive security mentioned above). Social issues are at stake to which the answer is technical solutions. "Where is the social responsibility and societal dimension?" one questioned. These types of solutions only seek to have control instead of trying to understand why they happen.

2.2. Morals

by IRKS

DESSI Tool Question	What is meant to be triggered with this question
Question 5) Does the security measure respect private zones, the right to private data etc.?	*Privacy is a fundamental right, which can be violated by for example surveillance or data-retention.*

Sector 1: Social and human science researcher communities

Scenario 1: One representative from **academia** raised a societal aspect: people do not always comply with surveillance. Therefore in scenario 1, bus drivers do not always agree with being surveilled all the time. Furthermore, so far there is no evidence that video surveillance improves security.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: Regarding data protection **industry representatives** raised the point that passengers are worried about being traced when data is generated in for example, busses. In general citizens are asking "Can I trust you? Where will the data be stored? I worry about data being stored in the cloud. Are technical measures sufficient for protecting our data?" There are questions and worries which industry representatives have to take into account. Another argument was that in some European countries recordings are not allowed outside the bus, therefore pictures can be pixelated to not monitor people outside public transport vehicles. Thus, we have to take into account different regulations in different European countries.

Scenario 2: An **industry representative** mentioned that human trafficking is a highly profitable business. Other than with dealing drugs, human smugglers are being paid in advance. Therefore, if the immigrant dies or if he/she reaches EU territory, there is not a big difference for them. Another industry actor argued that we don't have a data protection issue here because these immigrants are trying to enter EU and do not have a legal status with regard to data protection.

Sector 3: End-user
Sector 4: Security policy-makers
Sector 5: Civil society actors

DESSI Tool Question	What is meant to be triggered with this question
Question 6) Does the measure respect fundamental rights like freedom of thought, conscience, religion or expression?	Example: Censorship often violates the freedoms of expression.

Sector 1: Social and human science researcher communities

Scenario 1: A **social science representative** mentioned that the degree of respecting fundamental rights depends on the European Member State. For example, Austrians are more sceptical about video surveillance then people in other countries like the UK. Another representative from academia insisted that the question of whether a person should be under video surveillance is not a technological issue but rather a democratic decision. Another point that was raised was the lack of studies regarding public transport passengers' attitude towards video surveillance. Further research has to be conducted on this issue.

Scenario 2: Another **social science actor** argued that immigrants have the right to apply for asylum once they enter EU territorial waters. Theoretically, there is no legal basis for stopping immigrants from getting to the EU. At the end, it is less a security problem but rather a political and a human rights problem because the main question is who is taking responsibility for immigrants trying to enter EU (e.g., by sea) and who will save their lives. Another actor representing the scientific community argued that many irregular migrants are driven by economic motives. Nonetheless they are also eligible to apply for asylum status. However, a social science representative mentioned that the role of Tunisia and Egypt is to close their borders. Immigrants on the other side do not want finger-prints to be taken because of the Dublin Regulation which makes it impossible to submit multiple applications for asylum in different member states.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: An **industry representative** pointed out that a public transport vehicle, e.g. a bus, is closed and confined area therefore passengers cannot escape in case of emergency. The industry actor liked the idea that that there is video footage as evidence if an incident happens. However, the industry representative has never seen a study that states that passengers are against video surveillance.

Sector 3: End-user
Sector 4: Security policy-makers
Sector 5: Civil society actors

DESSI Tool Question	What is meant to be triggered with this question
Question 7) Is the security measure suitable, necessary and in balance with the problem (proportionality)?	Are the five sector representatives guided by different moral principles? ***Proportionality*** *is about balance between problem and measure.* ***Necessity*** *is about a rational need for intervention.* ***Suitability*** *is about solving the actual problem in a precise and appropriate way.*

Sector 1: Social and human science researcher communities

Scenario 1: A **social science representative** stated that there has to be a balancing of security and safety. For example, is there insurance for a bus driver when something happens? The same **academia** representative questioned if video surveillance has to do something with harassment, because it will not be able to prevent anything to happen. For this **science actor**, there is no relation between harassment and video surveillance. Another **social scientist** raised the question if video surveillance was ever evaluated related to violent incidents. Therefore, surveillance and usability are not always taken into account. Another **academia** representative asked how suspicious behaviour (deviant vs normal behaviour) is identified. One more argument regarding our current control system was that it is trust based. For example, a journalist accidently forgot a box when the Olympic Games took place in London. This incident ended up as a terrorist attack with 10,000 people being evacuated. In the end, it turned out to be false alarm.

Scenario 2: A representative from the **social and human science** researcher community mentioned that the EC funded project Autonomous Marine Surveillance System might interfere with fishing boats legally fishing in Tunisia and other African countries.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: An **industry actor** mentioned that regarding proportionality there are a lot of grey zones. Another industry representative (a business developer) raised the question whether installing CCTV cameras is a sustainable measure. A third industry actor stated that invisible CCTV surveillance could indeed be a suitable security measure because the perpetrator does not expect to be prosecuted. In his opinion, which was shared by other industry actors, the number of cameras installed does make a difference (having a camera above means getting a better overview of the scene). However, it is not a preventive measure in the first place. More cameras mounted in good position are effective according to his opinion. The same industry representative stated that a lot of light helps, too: people do not tend to get aggressive in well-lit environments. Another industry actor argued that having a driver in the spot light while driving during night has negative consequences too because the driver then becomes an exposed target and also for safety reasons this option seemed not to be interesting in the view of the industry representatives. Industry actors insisted that more cameras are needed in each bus. Audio surveillance would help identifying perpetrators.

Industry representatives mentioned also that there is a need to meet the driver's privacy expectations. Another suggested measure is audio intervention – it helps when audio signals are played not just in front but also in the back of the bus. The costs of a security measure also have to be considered as one representative from industry pointed out. Industry actors also mentioned that it is hard to measure whether video surveillance increases security. How to do it methodologically? Statistic evidence is hard to obtain. One argument was that bus drivers in some countries are threatened of being attacked every single day. Therefore, measures have to be taken to deal with

this problem. One industry actor raised the point that video surveillance has a preventive effect when passengers are confronted with their own picture upon entering the bus. Another industry representative mentioned that if the incident is outside the bus it is not his problem anymore. This actor does not care what happens outside the bus and if someone gets hit outside this terrain it is not considered to be her problem anymore. One more argument towards proportionality is that people are getting used to video surveillance. Some years ago people were very concerned about video surveillance, not using busses with video surveillance, nowadays it is the other way round: people do not want to use busses without surveillance cameras.

Another **industry actor** mentioned that we have to differentiate between perceived security and real security. How is it possible to measure it from industry perspective? A counterargument from another industry actor was that we are going towards technology nowadays and it is improving, e.g. facial recognition for pupils when entering the school bus in US already works. This argument was put into perspective from another industry representative with mentioning that there is always a human behind who has to make a decision. Therefore, technology is also vulnerable because humans are involved.

Another **industry actor** mentioned that in the future we are not going to need operators anymore. This opinion was not shared by other industry representatives, rather stating that humans will always be involved. Again, other industry actors did not agree on that. One representative was of the opinion that also automatized systems can learn (e.g. identify that a passenger forgot an umbrella). It was also argued by industry actors that these systems don`t work really well in daily use. There are still too many errors made by these systems.

Scenario 2: During the discussion on Scenario 2, one **industry representative** asked the question of how to best reduce migration pressure and answers it at the same time: By offering African countries better equipment for hindering boats with immigrants to start their journey to enter EU.

Sector 3: End-user

Scenario 1: An **End-user** argued that the operator is important in daily work. However, it is hard to say whether video surveillance prevents anything but the operator is the important person in charge. He decides when to send persons to an incident and when not. Threats at airports, for example, are higher in general than at public transports.

Sector 4: Security policy-makers

Scenario 1: A security **policy maker** argues that it is in the interest of any particular country's government to be well protected. However, yet it is not clear whether video surveillance improves security. This representative mentioned that we only want to see the perpetrator, but there are a lot of other people too at the airport. For example, at airports we have to reduce the amount of false alarm to less than 10 %, otherwise it is not usable.

Sector 5: Civil society actors

2.3. Cultural Ideals

by KCL

DESSI Tool Question	What is meant to be triggered with this question
Question 8) Does any involved processing of personal data conform with data protection regulations?	Are the sector survey representatives aware of potentially necessary data protection implications of the proposed measure?

Sector 1: Social and human science researcher communities

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: **Security industry** actors have voiced a number of ideas and values relating to this issue of data processing and data protection. The cost of ensuring data protection was mentioned in relation to the necessary destruction of tapes in the case of CCTV recording. Also, the question of anonymity seems to retain some importance. Are we speaking of the passengers' or the driver's anonymity? While the former seems to be of lesser importance to security industry actors, the later look arguably more important – which may be indicative of the memory of social tensions with the workforce, with which industry actors have had to deal with while deploying their CCTV products within transport firms. At any rate, technical solutions, such as pixellisation, are offered with the hope to strike a proper balance between anonymity and security. This should not, however, obscure the fact that a powerful drive towards "breaking anonymity" informs the claims made by security actors in the case of handling personal data. Security industry actors with a background as end-user are aware of the fact that ensuring anonymity through anonymisation of the data is a dead-end, because it is always possible to track the origin of the data (chain of evidence).

Sector 3: End-user

Sector 4: Security policy-makers

Sector 5: Civil society actors

DESSI Tool Question	What is meant to be triggered with this question
Question 9) Is the security measure resistant to use that goes beyond its original approved purpose?	Where does function creep begin? Is it possible to instrumentalise function creep politically? Is there a different sensivity for function creep along the five sectors? *Technology and systems can be reshaped or reused for new purposes, which they were not approved for. This can be intended (misuse) or sneak in over time (function creep). Resistance to that can be built into the technology or the way it is administered.*

Sector 1: Social and human science researcher communities

Scenario 1: Representatives of this sector have made some observations relating to the possible instrumentalisation of CCTV cameras for the reinforcement and stepping-up of the managerial coercion of the workforce. It is the bus driver who may end up under surveillance, instead of potential trouble-makers.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: **Security industry** actors display a wide variety of stance on this issue, depending on their particular background. Security industry actors with a background in computer science immediately raise the point that any data recorded by any device may be used for purposes other than those originally intended (function creep). The problem is particularly apparent with video surveillance, for it may allow the tracing of individuals by adding one more trace into the system.

Other actors of the security industry recognize this reality of this problem. In response to the claim of social and human science researchers that video surveillance may be used to enhance managerial coercion on the workforce, they oppose a counter-claim that such surveillance may, in the end, help drivers sustain their own claims in the case of heated argument with passengers, and that consequently, video surveillance protects drivers against passengers.

These actors also insist that recording images of people does not hurt as long as images are not misused. They propose some technological arrangements to decrease the possibility of potential misuse, but leave it to their clients to decide exactly how resistant the technological solution has to be against misuse. It is worth noticing that these actors think in terms of misuse, and not terms of function creep.

Sector 3: End-user

Scenario 1: **End-users** candidly acknowledge the reality of function creep in the sense that they implicitly reject the generated accepted discourse of justification in terms of deterrence and prefer to see video surveillance as a more operational way to investigate incidents once they have occurred.

Sector 4: Security policy-makers

Sector 5: Civil society actors

DESSI Tool Question	What is meant to be triggered with this question
Question 10) Does existing regulation sufficiently cover the use and effects of the security measure?	Which sector representative is in favour or against additional legislative measures? Which sector representative is referring to state control functions? *If new procedures or new technology are introduced, the legal framework may need to be adapted. Does the legal framework live up to the demands imposed by the security measure?*

Sector 1: Social and human science researcher communities

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: **Security industry** actors made a number of observations on the relations between law and security. In the case of video surveillance, it was mentioned that the security device does not articulate well with law, for the incidents that it aims at suppressing are qualified by law neither as criminal offences nor as misdemeanours.

Scenario 2: These actors readily recognize that law sets up the general conditions within which not only security devices but also security technologies are to work. In the case of ensuring border security in the Mediterranean, obligations to respect international law were recalled many times in terms of non-refoulement of asylum-seekers or non-use of drones to monitor large maritime areas.

Security industry actors with a background as end-user also underline that law actually impedes border guards from doing their job, which is to prevent foreigners to enter a country. Given this general condition, border guards are left with no choice but trying to know who is entering the country

Sector 3: End-user

Sector 4: Security policy-makers

Sector 5: Civil society actors

DESSI Tool Question	What is meant to be triggered with this question
Question 11) Does the security measure foster trust and confidence between people?	*Some security measures create distrust, separation and fear within society. Do the sector representatives reflect on that fact?*

As a general observation, it should be underlined that, in the case of the video surveillance -scenario, all of the participants have readily accepted the premise that the aim of video surveillance is to discipline and punish groups of youngsters using public transportation, sometimes while being drunk – although the moderator has made it clear during the presentation of the solutions at hand that the "broken-nose" scenario was a very seldom event and, on the top of that, the perpetrators of these incidents are unknown. The fact that the entire discussion has proceeded under this very specific, and questionable, assumption indicates a cross-sectorial trends towards generational mistrust of youngsters in urban environment. Youngsters are for the sector representatives per-se under suspicion to be trouble makers that cause security problems.

Sector 1: Social and human science researcher communities

Scenario 1: **Social scientists** have voiced concern about the fact that highly-technological and visible security devices may have advert consequences on trust-based social systems by signalling that individuals are suspect by definition and should therefore be kept under surveillance. They have also underlined the fact that security systems may unsettle security norms in terms of solidarity in case of aggression, by displacing the responsibility to intervene not on passengers and by-sanders, but on the control centre. Since security systems operate in specific cultural context that may vary widely, it is very difficult to predict what kind of consequence a given security device will have on such deeply sedimented cultural and social patterns of behaviour.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: **Security industry actors** proceed under the claim that a minority of troublesome individuals are inherently aggressive. They consequently cannot be trusted and, instead, must be kept under close surveillance by the means of security devices. Undergirding their argument is a claim that security devices will not be able to suppress this kind of aggressive behaviour, but may however be successful at moving it away from certain places – such as public transportation. Threat is therefore perceived as a potential that may actualize in any given place, at any given time. Security devices are used to target the actualization of this potential on specific places and at specific times. In selling the security devices that they manufacture, actors from the industry tend to over-emphasize widely the kind of behaviour that is at stake.

The relation between security and trust comes in under a second, a related claim. Those who are to be monitored do not trust governments and public institutions, so any softer interventions are doomed to fail. Arguably, this opens the way for hardening of security dispositive.

Scenario 2: Actors from the security industry voiced concern about the costs in terms of human lives of hardening border control in the outskirts of Europe.

Also, they have pointed to a cultural ideal whereby people can choose to stay where they are and do not have to start crossing international borders at the peril of their life in search of a better, of even decent, standard of living.

Sector 3: End-user
Sector 4: Security policy-makers
Sector 5: Civil society actors

2.4. Social Norms

by TNO

DESSI Tool Question	What is meant to be triggered with this question
Question 12) Does the security measures introduces new risks, and if so, are these acceptable?	*New risks may be introduced - for example the risk that a new security glass breaks down and hurts someone. Are there such new risks? If so, the risks compared to the benefits may be evaluated with regard to acceptability.*

Sector 1: Social and human science researcher communities

Scenario 1: Youngsters have the tendency to overreact, so they may feel invited to act violent.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: There are many ways to protect the data so that only in case of an important incident the pictures will be taken. Another industry representative was in general critical to data collection and protection. But on the other hand, as a passenger the representative would tend to appreciate it. It would give a more secure feeling. The representative could not say whether retention of the data

would be a concern. But as an industry representative it was a relevant [argument for being careful in introducing data collecting technologies – MHV].

If the clients of the representative are governments, how can industry as a provider protect against misuse? They will not sell their products to all governments, they will check how they intend to use the data.

Another industry representative was not sure whether industry has an issue here at all. It is in the full responsibility of their costumers to mitigate risks, the industry doesn't sell products/services that generate new risks. Risk is always man-made and not introduced by technology; technology is always "neutral".

Sector 3: End-user
Sector 4: Security policy-makers

Scenario 1: If you install a technological measure, it is always a signal: e.g. place is not secure, so we had to do something about it.

Sector 5: Civil society actors
Scenario 1: Cameras may replace the feeling of responsibility. There are CCTV surveillance cameras, so I do not have to react to the situation. Technology makes experiences different. What do we teach our children? Do we teach them to trust on technology or to think for themselves?

DESSI Tool Question	What is meant to be triggered with this question
Question 13) Is there enough knowledge about the security measure to make a rational decision possible?	*There are two aspects in this criterion: lack of general knowledge about the technology used, or lack of concrete information on implemented technology because the alternative is not specified enough.*

Sector 1: Social and human science researcher communities

Scenario 1: There is not enough data/knowledge available to come to a decision, if a measure is useful or not in that particular context (demand for more research/knowledge before deciding). Some measures may increase the perception of security, but not actual security, sometimes organisations play security theatre just to increase a perception, but if you look closely at the development of the number of incidents reported to/by the system they want to implement one does not see a clear need for (yet) another security measure to be implemented at all.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: Sometimes the quality of the data (e.g. pictures, profiles, etc.) is too poor to be used by law enforcement agencies (LEA) so they don't know whether a measure was effective. The industry representative said that if one thinks of the possibilities of new technologies such as HD cameras one would see a clear benefit. Technology is developing rapidly, what was a standard 10 years ago is now by far an out-dated technology, so there is a progress in this field.

Basically the job of the industry is to make sure that the system is working, otherwise it would not sell so many devices, so the question, whether or not there is enough knowledge about a security measure does not concern them that much, of course they have to convince their clients through the products they provide.

Sector 3: End-user

Scenario 1: In industry's understanding the field operator is a crucial factor in interoperating the data collected by the technological devices the industry provides them with. It is the human being that selects and decides on further actions based on the evidence gathered through technology, so you still have this human factor, which is important to acknowledge when thinking about a new measure to be implemented.

Sector 4: Security policy-makers

Scenario 1: Does more technology solve more crimes; prevent more incidents, who knows? One problem is though - what if you have so much information about a certain technology, how do you handle this circumstance?

Scenario 2: The question is not whether the technology can do it; the question is what you do with those vessels that are detected by the system. If you think from a border control perspective, than you want to stop these people coming to my country. What you do in the scenario, is not clear. If you

encounter them you might not be able to stop them, however next time you may have the information who they are and where they come from, etcetera. You get a picture about it.

Sector 5: Civil society actors

Scenario 1: There are social issues at play. And we are putting in place a technical solution. And there is no good empirical evidence that video surveillance really decreases the number of incidents. Where is the social responsibility? It is all about the control. Not about understandings.

DESSI Tool Question	What is meant to be triggered with this question
Question 14) Are risks and benefits distributed fairly?	What is regarded as a (reasonable) risk for a sector representative? *Is it considered that a certain activity can endanger specific societal groups such as risk groups, i.e. persons who are vulnerable to a higher degree or do not have enough capacities to cope with certain risks.*

Sector 1: Social and human science researcher communities

Scenario 1: Security has different implications for different groups in society. What is the security for one group (the bus drives in scenario 1) may be the insecurity for another group (the passenger in scenario 1).It always depends on the socio-cultural context, if a measure is perceived to increase security. In some countries in Europe citizens are rather sceptical about data gathering measures in contrast to other countries. Sometimes side-effects of security/surveillance technology are not considered thoroughly. On the example given in scenario 1 one could think of the camera's also as a means to surveille the bus drivers performance and not only to prevent future incidents of vandalism or violent behaviour by passengers.

Sector 2: Security industry actors (incl. technology developers)

Scenario 1: It is always a question of whose security is to be concerned. We should look at the overall effects, of course. For example in the U.S. parents can get a picture of their child on their smartphone, when the child enters the school bus, as industry we have a challenge there as for European standards that would probably go way too far.

Sector 3: End-user
Sector 4: Security policy-makers

Sector 5: Civil society actors

Scenario 1: One has to be careful about different solutions and their precise implications. And, the question is who needs to be protected? In England the passengers needed more protection. It is about a threshold, first there was one camera, later on there will be ten maybe, we have to be careful not to militarise every spot/place in our lives. There are social issues at play. And we are putting in place a technical solution. And there is no good empirical evidence that video surveillance really decreases the number of incidents. Where is the social responsibility? It is all about the control. Not about understandings and you should not forget about your fundamental right of a private live.

2.5. Political Priorities

by FhG INT

DESSI Tool Question	What is meant to be triggered with this question
Question 15) Does the security measure improve the relation between state and citizens?	Be aware of the importance of trust between general public and state (government, authorities, etc.). *The existence of the state embodies a delegation of power from free citizen to the state, by which the citizen gives up some autonomy. In exchange for that, the state delivers collective services in terms of, for example, democracy, protection against enemies, a basic supply of food and water, healthcare, an education system etc. This bargain between the state and the citizen rests on the trust that the state will not misuse the delegated power. Any change in the power delegation, in the trust or in the services that the citizen can expect, indicates a shift in the relationship.*

Sector 1: Social and human science researcher communities

Trustworthy security measures in a technical sense (i.e. effectiveness, low false-alarm rates etc.) may destroy existing trust systems

Sector 2: Security industry actors (incl. technology developers)

Empowerment of citizens to avoid escalation levels up to police.
Security measures as deterrent to direct people's behaviour in a desired direction.
Public security personnel develop in a direction where they ask more and more for equipment that protects themselves (after strongly objecting it in the past).
Comparisons with security practices elsewhere (e.g. US) in order to relativise disproportionate measures.

Sector 3: End-user

Even if measures appear reasonable at first glance, their further consequences and actual contribution to the solution of the problem have to be thought through.

Sector 4: Security policy-makers
Sector 5: Civil society actors

DESSI Tool Question	What is meant to be triggered with this question
Question 16) Does the security measure improve democratic participation and means of exercising political rights?	*Being able to exercise participation is one of the main pillars in democracy. It includes the rights to meet, engage in public political discussions, to become member of a political party, to stand up for election and to vote in elections. Further, it involves the democratic participative culture of contributing to the management of our societal institutions by for example involving oneself as citizen representatives in public boards or attending and contributing to civic meetings or even protesting. To what extent does the security measure change the width and depth of such democratic participation by political actors and citizens?*

Sector 1: Social and human science researcher communities

Proportionality of measures is a democratic issue and should not be discussed by technocrats. Security measures often give the general public the opportunity to give responsibilities to someone else.

Sector 2: Security industry actors (incl. technology developers)

Sector 3: End-user

Sector 4: Security policy-makers

Sector 5: Civil society actors

DESSI Tool Question	What is meant to be triggered with this question
Question 17) To which extend do I assess people's opinions (lay people), participation and ability to discuss?	*The criterion rests on the idea that experts should deliver facts and insight and lay-people (including politicians) should judge value questions, such as answering the question of the acceptability of insecurity or security measures. This criterion also addresses the institutional power of security actors (intelligence services; security industry; police and military) on the one hand and alternative approaches to security (mediators in society; humanitarian organisations; peace-movements) on the other.*

Sector 1: Social and human science researcher communities

The general public (EU in- and external) should not be assessed as uninformed or irresponsible of their actions.

Sector 2: Security industry actors (incl. technology developers)

The general public does not know about privacy/civil rights enhancing features of security measures.

Sector 3: End-user

As long as the citizen does not realise that his rights got infringed upon, it is not a real problem.

Sector 4: Security policy-makers
Sector 5: Civil society actors

2.6. Economics

by Tecnalia

Scenario 1: General remarks on how Economics came to play during the discussion on scenario 1: The very first question which was asked after the presentation of the first case (public transport) was about the limitations of the budget by the **industry representatives**. Although economic restrictions were not established as an important criteria the option to cast extra light around the driver was presented an effective and the same time low cost solution. Some **industry representatives** compared again later in the discussion the costs and effectiveness of the different options of video surveillance. **End-users** stated that when less passengers use the bus services the company may suffer some economic loss. In this context it is mentioned that the company would try to keep the problem "outside of the vehicle".

Industry representatives (retailers and representatives from the professional association) argued that in this particular case of public transportation and related security problems the operating company cannot be held responsible for larger societal security problems. The representatives from academia and civil society didn't share the same opinion and argued that it is in fact within the responsibility of the industry to address problems on a larger scale. No consent was achieved in this discussion. For the industry representatives a security problem is only of relevance as long as it is within their system of reference (= the operating system, the branch, the company), as soon as a transfer to another area of responsibility can be achieved, the problem (for the industry) is solved whether or not it still exists on a larger (societal) scale. "Why should we pay for problems that result from other causes we are not responsible for …"

The conversation changes to customer satisfaction and its relation to the demand of the bus service. It is argued that independently from the conflictive feelings that CCTV creates in different people, these are not likely to change the consumer behaviour (**Policy Maker).** The discussion moves to the positive and negative costs of CCTV and the need for assessment for decision-making. Less human intervention (marshals) and more video surveillance would have economic advantages (**End-user**). It is suggested that video surveillance would decrease cleaning and maintenance costs (**Policy Maker).** ROI for video surveillance is about 18 months, it should be considered as a cost saver as a bus driver on a sick leave supposes additional costs for the company **(Industry Representative).** Although there is no statistical data, it is again mentioned that video surveillance would prevent damage **(Industry Representative).**

Scenario 2: General remarks on how economics came to play during the discussion on scenario 2: It was argued that immigrants have paid high price to smugglers to make the journey to Lampedusa, even so, they don't have 40 euros to pay for their visa (**Industry Representative**), on the other hand applying for a visa to Europa could help to avoid the high costs of illegal immigration. Another **Industry Representative** states the trend of the states to spend less money on international security and more on home security.

3. Observation on the interaction between the sector representatives

In addition to the modes of interaction in the different security claims (e.g. security values, morals, cultural ideals, social norms, political priorities, economics) attention was also paid to the interaction of the participants on a more general level. The aim was to learn whether they understand each other, if there was e.g. too much "technical talk", if they try to see the point of view of the other participants or if the live in different "thought worlds".

This was done by applying two different methods. First, participants were observed during the role-play in the two different scenarios and second we asked the participants to fill out a questionnaire about their experience in interaction with representatives of other sectors. For the observations of the role-play as well as for the questionnaire we have created a set of different types of "difficulties" people could experience during interactions like meetings, workshop or other forms of cooperation.

1. **Incompatible ideology or philosophy of life**
    - *(e. g. members of the different sectors live in different "thought worlds")*
2. **(Wide) discrepancies between yours and the discussion partner's professional needs and requirements**
    - *(e. g. issues are perceived differently or are lacking mutual acceptance and/or understanding)*
3. **Difficulties due to different time horizons playing a role in different sectors**
    - *(e. g. short term versus long term goals)*
4. **Difficulties due to different organisational or bureaucratic conditions**
    - *(e. g. modes of publication, quality management, financing, corporate culture, etc.)*
5. **Difficulties to understand each other at a technical level**
    - *(e. g. based on different professional backgrounds)*
6. **Difficulties due to different national or cultural backgrounds**
7. **Discussions tend to get heated and emotional; it is difficult to discuss issues objectively**
8. **Other language difficulties**
    - *(e. g. based on different proficiencies of the English language)*
9. **Difficulties tend to be at a personal level / personal dislikes**

Figure 1: Different types of difficulties one could experience, when interacting with representatives of other actors.

3.1. Observations in scenario 1 – "Security in Public Transport"

At the beginning of the role-play the main interaction between the attendees took place between the invited participants and the moderators. Questions were asked to specify the security problems and the participants themselves gave explanations or insights into the presented security challenge. The interaction was generally very cooperative and several affirmative idiomatic phrases like "I fully agree", "absolutely right" or "he/she said a valid point" were used. The participants acted as a team, ready to share their different professional background to solve a security problem.

The first difference in the point of view could be observed when the question "Do CCTV cameras help to prevent incidents" arouse. The participants were endeavoured not to destroy the harmonious atmosphere by using "I messages" (e.g. "I like it when there is a camera") or formulate it as a question (e.g. "Is it out of proportion?").

The discussion got slightly more emotional when the pros and cons of CCTV cameras were discussed between representatives of the industry sector and CSOs (security value versus privacy). But in general the industry representatives seemed to have a lot of experience in dealing with these sorts of conflicts, so that they used many forms to de-escalate the conflict (e.g. "it's a fair statement", "we can talk about it", "I respectfully disagree"). On the other hand, the little laughter from time to time showed that although the participant is well trained in dealing with conflictive situations, he is also somewhat irritated to undergo the same discussions again and again. In the end no common position was reached, but both sides (industry and CSO) emphasized their willingness to engage in further dialogues.

Other different point of views during scenario 1 (data protection – how to handle the recorded material) were discussed objectively. The participants simply exchanged their expertise in this area.
It could be observed that many of the participants were used to discussions about the value of CCTV cameras in general ("we all know the discussions about CCTV"), they knew the arguments and were well trained to stay on professional level and not to get too emotional or even aggressive.

3.2. Observations in scenario 2 – "EU Border Control"

During the discussions about scenario 2, it became clear that all the participants shared more or less the same understanding regarding the autonomous marine surveillance system. Thus, the interaction mainly took place between the participants and the moderator (regarding details of the scenario) and between the participants and an expert of the situation in Lampedusa (regarding the legal, political and humanitarian situation). As the point of view of the participants did not differ much, the general interaction was rather constructive and consisted mainly of a knowledge exchange between experts with different professional background. The security challenge was seen as a problem without (an easy) solution, thus the scenario did not lead to a situation where the advantages and drawbacks of a specific solution were discussed. In general the conversation took place in a structured, polite and cooperative way.

3.3. Summary

Generally it was observed that the interactions between the participants developed in a friendly atmosphere. The attendees acted like a team in which the different professional backgrounds were valued and the knowledge exchange was paramount. Even during discussions in which the point of

views seemed to be rather incompatible, the participants tried to uphold an open-minded atmosphere and to be responsive to one another. However, a common solution was not reached.
However, one has to take into account some points which heavily supported this friendly atmosphere:

- The security challenge which was presented to them was not *their* problem. Although they might have experienced similar challenges in their day-to-day work, the scenario still was not a problem they felt responsible for (because it was already solved (scenario 1) or because it was out of their sphere of influence (scenario 2)
- Most attendees had long years of experience in either the field of CCTV cameras or migration & border security. Thus, they knew all the advantages and drawbacks of possible security solutions and had much experience in looking for compromises and common solutions.
- Most attendees had also much experience in interacting with people from other sectors. Thus they were trained to de-escalate possible conflicts and be responsive to different point of views.

However, the situation could be rather different, if a group of people with different professional backgrounds has to solve a real and new problem. In a group with unknown participants, with experts who rarely have the possibility to work in an interdisciplinary team and with a security challenge they are not familiar with, the situation could be completely different.

To get an impression of the situation in the day-to-day work of the participants of the workshop, they were asked additionally to fill out a questionnaire, how they experience the interaction with participants of other sectors in their daily work. For each sector (social and human science researcher, technology developer or security industry actor, security technology end-user, security policy maker, civil society organisation) they were asked to tick one or more of the different possible types of difficulties during an interaction as mentioned in Figure 1. The result of the filled out questionnaires (9 overall) are presented in Figure 2. Although the number of questionnaires is rather low, some issues still can be pointed out. The main problem when interacting with representatives of other sectors seems to be that these “others” seem to have a different philosophy of life and live in different “thought worlds”. On the other hand, difficulties on a personal level or (too) emotional discussions were rarely mentioned.

To get a sounder picture of possible difficulties during interactions, the consortium will publish an online questionnaire containing similar questions and will disseminate it to a wider public. The results of the online survey will be published in D2.4.

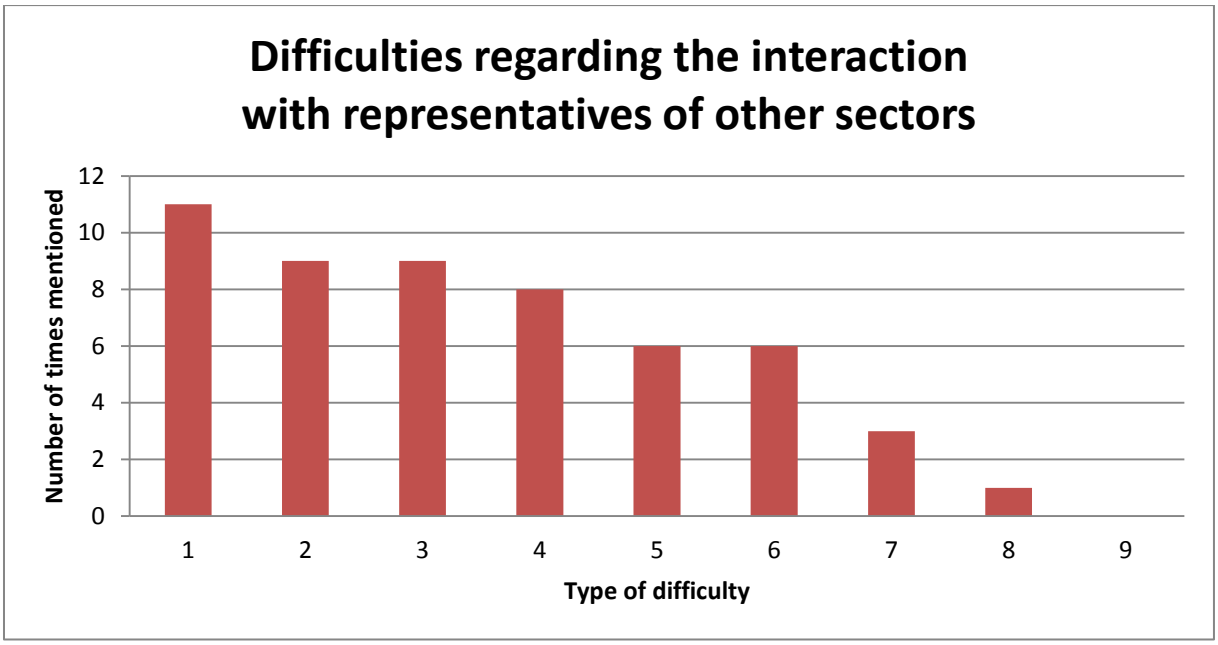


Figure 2: Difficulties regarding the interaction with representatives of other sectors

1 - Incompatible ideology or philosophy of life; 2-(Wide) discrepancies between yours and the discussion partner's professional needs and requirements; 3 - Difficulties due to different time horizons playing a role in different sectors; 4 - Difficulties due to different organisational or bureaucratic conditions; 5 - Difficulties to understand each other at a technical level; 6 - Difficulties due to different national or cultural backgrounds; 7 - Discussions tend to get heated and emotional; it is difficult to discuss issues objectively; 8 - Other language difficulties; 9 - Difficulties tend to be at a personal level / personal dislikes.

4. Concluding remarks

4.1. The good, the bad and 'it's complicated'

The DESSI method that was applied to create a methodological framework and to structure the discussion forced the participants to decide whether a concrete measure that was presented in a security scenario should be assessed positively or not. While particularly discussing the effects of using video surveillance, the participants were divided in their opinions. During the discussion it seemed that opinions of the sector representatives were changing while additional issues and side effects were evoked. The problem seemed more complicated and did not have just one answer.

In general there was a disagreement between sectors and between members of the same sectors as to whether video surveillance really has a positive effect on improving security. Civil society representatives took a strong position that a video surveillance solution will not change the security situation in any measurable way. Social researchers pointed out that it was necessary to investigate whether video surveillance has been effective in the past before adopting it as a security measure. Some industry representatives argued that the sustainable effects of cameras have never been fully investigated. Other industry representatives disagreed and gave an example of a test in a city where some buses had cameras and others not, showing significant differences in results, in favour of the video surveillance. The policy-makers remained undecided but stressed the point, that although an evaluation as suggested by the scientists would be helpful is in their experience not always a possible solution, as soon as a technology is implemented and running it is almost impossible to take this solution down afterwards, therefore all this considerations have to be made in advance.

There was a general agreement between all the sectors that technologies that don't gather data are less problematic then those who gather information about citizens. Although industry actors argued that this is the 'price one has to pay' to live in a more secure environment and that the industry of course follows all national and international regulation when it comes to collecting and processing data about individuals.

For civil society actors and representatives from the scientific community it was pretty obvious that unless one has sufficient knowledge about all potential implications a security measure, might it be of technological nature or a more organisational or social measure, it is not possible for policy makers to decide if the measure is beneficial or not.

For the End-users and policy makers the picture is different though. Of course side effects have to be considered as suggested by the scientific community and the civil society actors, in practical terms it is always a question of resources how much time and money can be spent to evaluate and assess the potential threats that can be caused by a security measure.

4.2. Truth is what can be measured

As the first point of the concluding remarks refers mainly to the demand for more knowledge (raised by civil society actors and scientific community representatives) the second point is also about knowledge. While discussing the pre-defined security scenarios one could observe how all sides where referring to statistics that should proof their arguments. While particularly the civil society actors where not convinced by the statistics the industry representatives brought up during the discussion at all, the other sector representatives (namely End-users and policy makers) seemed to

be more convinced by statistics and studies that were mentioned during the discussion. Interestingly the scientific and civil society community is on the one hand questioning the effectiveness of security technology because of the lack of data, on the other hand as soon as a study is quoted that proofs the questioned effectiveness the sampling size or the quality of the study is questioned again. For End-users and policy makers these detailed questions on how the figures were measured seemed not to be convincing, as soon as an argument can be quantified and a percentage can be provided it seems to be more convincing than purely qualitative arguments that were brought forward during the discussion.

4.3. Side effects

The more time the discussants spent on one specific topic the more side effects of the measures discussed where discovered. While the industry representatives stressed points that would help to reduce costs, reduce the "human factor" as potential source of error or improve on the one hand they also addressed that the security industry as such can't be made responsibly for negative consequences as they see themselves at first instance as providers. A popular argument was if a technology is been sold to a government how can the industry assure the government is not misusing the technology against the citizens that should initially be protected?

The D2.3 report on the sector survey meeting will be analysed in the following D2.4 report and set the basis for the further development of the SOURCE network.

Annex I: Agenda of the meeting

Information for SOURCE consortium members participating in T2.3 Sector Survey Meeting in Brussels on June 5, 2014

1) Structure of the SOURCE sector survey meeting on June 4 - 5:

The SOURCE T2.3 sector survey meeting will start at 11.30 on June 4 (Wednesday) and end at 16.15 on June 5 (Thursday). The aim of the first day (June 4) of the meeting is to familiarize SOURCE partners involved in T2.3 and T2.4 with the concept of the workshop, rest run the workshop setting and simulate your role in the meeting. Therefore, only SOURCE partners will attend the first day of the meeting (June 4). Furthermore, we will have a workshop dinner (at 19.30 at the Restaurant MILLESIME) with all SOURCE partners involved and the external participants (representing different sectors of societal security).

However, during the second day of the meeting (June 5) the workshop with the external experts will be conducted. The aim of this meeting is to generate data and conceptual knowledge about the available modes of interaction between the five different sectors (social and human science researcher communities, end users, security industry actors, security policy-makers and civil society). The data generated in this workshop (T2.3) will be documented in the D2.3 and then be analysed by Task 2.4 partners. The concept of the workshop is jointly developed by IRKS and FhG INT and the workshop will be moderated by IRKS. D2.3 will be a descriptive report on the outcomes of the workshop in Brussels.

Other than indicated in the SOURCE DOW (part A, page 12 of 46) there will be just one sector survey meeting for T2.3 because accidentally no budget was planned for T2.3 meetings.

2) Agenda of SOURCE T2.3 sector survey meeting on June 4 and June 5:

Day 1: 4th of June 2014: **Introducing the SOURCE consortium members to the concept of the T2.3 Sector Survey Meeting and test run the workshop setting** (SOURCE internal meeting)

Time	Topic
11.30 – 12.00	State of play in WP2 by PRIO
12.00 – 12.30	Intertwining between Task 2.3 (data gathering) and Task 2.4 (data analysis) by IRKS and FhG INT
12.30 – 13.00	*Lunch Break*
13.00 – 14.00	Introduction into the workshop concept by IRKS
14.00 – 14.15	*Coffee Break*
14.15 – 17.00	Test run of the sector survey meeting by using templates and voice recorder (all partners involved in T2.3)
17.00 – 18.00	SOURCE Steering Committee
19.30	Workshop Dinner at the Restaurant MILLESIME

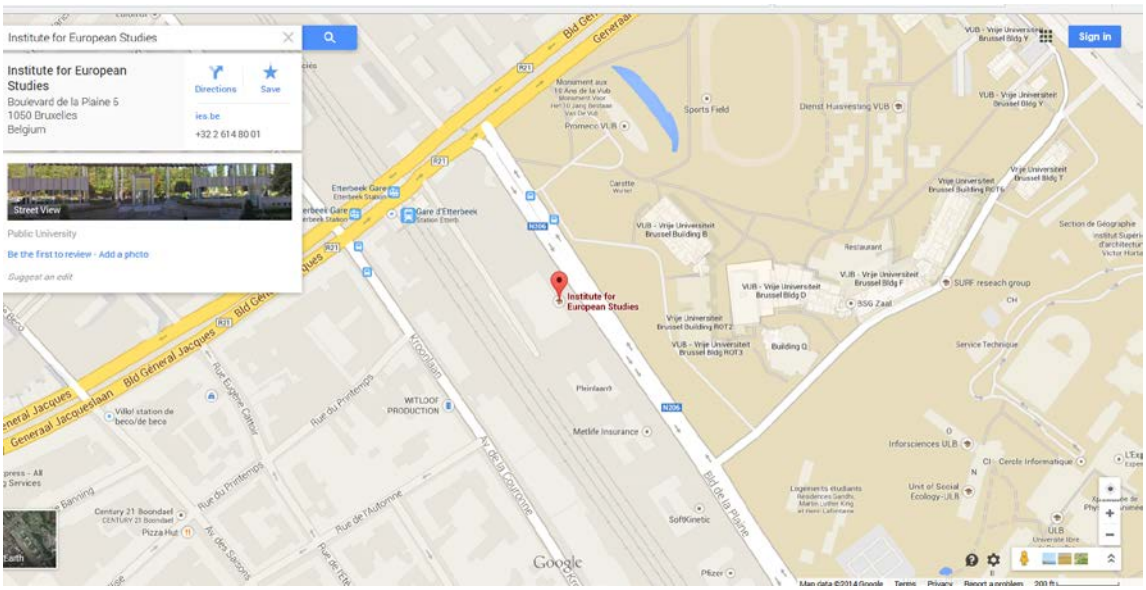
(Rue Eugène Cattoir 5 - 1050 Ixelles; Tel: +32 2 649 82 62;
http://www.restaurantmillesime.be/index.cfm?langue=en)

Day 2: **5th of June 2014**: **Running of the T2.3 Sector Survey Meeting with external participants** (external meeting)

Time	Topic
9.00 – 9.30	Introduction to the SOURCE NETWORK by PRIO
9.30 – 10.15	Introduction to the DESSI method by IRKS
10.15 – 10.30	*Coffee Break*
10.30 – 12.30	Workshop on Security Scenario 1: Public Transport
12.30 – 13.30	*Lunch Break*
13.30 – 15.30	Workshop on Security Scenario 2: EU Border Control
15.30 – 15.45	*Coffee Break*
15.45 – 16.15	Conclusions: Lessons learned today, discussion, feedback, etc.

3) Venue of the SOURCE sector survey meeting

Institute for European Studies, Conference Room Rome (Floor -1), Karel Van Miert Building Pleinlaan 5, 1050 Brussels . The venue is nearby the train Station Etterbeek (see map below).



Contact Information (for any additional questions or in case of any emergency situation):

Dr. Meropi Tzanetakis
Mobile: +43 650 920 1495
Email: meropi.tzanetakis@irks-research.eu

Mag. Alexander Neumann
Mobile: +43 650 306 5900
Email: alexander.neumann@irks-research.eu