SECONOMICS

D4.3 Communication patterns and effective channels of communication

P. Guasti, Z. Mansfeldová, J. Hronešová, D. Gawrecká, P. Vamberová, T. Lacina (IS AS CR), U. Turhan (AU), A. Tedeschi (DBL), M. de Gramatica, W. Shim (UNITN), J. Williams (UDUR)

Pending of approval from the Research Executive Agency - EC

Document Number	D4.3
Document Title	Communication patterns and effective channels of communication
Version	1.0
Status	Final
Work Package	WP 4
Deliverable Type	Report
Contractual Date of Delivery	30.4.2014
Actual Date of Delivery	30.4.2014
Responsible Unit	IS AS CR
Contributors	DBL, ISST, ATOS, URJC, AU, UDUR, UNITN
Keyword List	communication, risk, security
Dissemination level	PU

SEVENTH FRAMEWORK PROGRAMME

Security Economics: Socio economics meets security

SECONOMICS Consortium

SECONOMICS "Socio-Economics meets Security" (Contract No. 285223) is a Collaborative project) within the 7th Framework Programme, theme SEC-2011.6.4-1 SEC-2011.7.5-2 ICT. The consortium members are:

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESCHI Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	1495 UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Dr Matthew Collinson matthew.collinson@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	AtoS	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Alicia Garcia Medina alicia.garcia@atos.net
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr Ruprai Raminder Raminder.Ruprai@uk.ngrid.com
11	ANADOLU ÜNİVERSİTESİ	ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION Iki Eylul Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr
12	Durham University	The Palatine Centre, Stockton Road, Durham, DH1 3LE, UK	Contact: Prof. Julian Williams julian.williams@durham.ac.uk

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	31/05/2013	Draft	Z. Mansfeldova, P. Guasti (IS AS CR)	Table of content
0.2	02/07/2013	Draft	A. Tedeschi (DBL)	Contribution to the draft
0.3	28/02/2014	Draft	Z. Mansfeldová, P. Guasti (IS AS CR),	First draft
0.4.	10/03/2014	draft	P.Guasti, Z.Mansfeldova (ISASCR)	Draft
0.5	25/03/2014	draft	M. de Gramatica, E. (UNITN)	Suggestions and feedback
0.6	26/03/2014	draft	J. Williams (UDUR)	Scientific review, minor Comments
0.7	15/04/2014	Draft	P.Guasti, Z.Mansfeldova (IS AS CR),	Final draft
0.8	17/04/2014	Draft	E. Chiarani (UNITN)	Quality Check. Some changes and remarks in the formatting
0.9.	23/4/2014	Draft	W.Shim (UNITN)	Quality Check, scientific review, minor comments
1.0	29/4/2014	Final	P.Guasti, Z.Mansfeldova (IS AS CR),	Final Report

INDEX

Executive summary

This deliverable combines qualitative and quantitative survey methods to provide an analysis of communication channels and patterns between policy makers, stakeholders (i.e. companies), and citizens in the areas of security and risk in regards to three specific areas of critical infrastructure – air transport, public transport, and CNI.

Based on the literature of political communication, we first propose a new theoretical framework for the comparative study of communications in the field of security. We then provide an overview of the media landscapes in the countries under study, paying special attention to the national and international context and its changes over recent years. In order to further validate the use of media for our analysis, we analyse public trust in the media and confirm that, due to high trust and the high salience of security issues in the media in recent years, the media offers a good subject for the comparative study of the difficult balance between security and freedom.

In the third section, we define salience as a tool for studying communication within security. The fourth and most important part of the deliverable, the analysis, studies salience within the domains of airports, critical infrastructure and public transport.

In the case of airports, we have identified that the three most important factors that affect the salience of a security measure is the nature of the security measure itself, the explanation of the security measure provided to passengers by airport authorities, and finally the amount of attention paid by authorities to passengers' perception and acceptance of measures. In an age when air travel is increasingly open to passengers of various ages and social and cultural backgrounds, the challenge for security authorities is recognizing and addressing the diverse needs of these passengers in communicating and providing security, whilst acknowledging and respecting the needs of passengers.

In regards to critical infrastructure, we highlight the specific character of this debate. The media's discussion of Stuxnet was very important, as it was the first transnational debate of cyber-attacks and cyber warfare. The salience and resonance of Stuxnet also highlighted the degree to which cyber threats can affect the everyday activities of citizens, such as online communication, sharing information via social networks, internet banking, paying with credit cards, etc.

In respect to public transport, we find that, first, CCTV cameras have high positive salience and are thus an enthusiastically accepted crime-prevention measure. Second, considering public transport passengers most frequent complaints, CCTV is the best instrument to mitigate these problems. Third, overall we find low negative salience, i.e. few complaints. Fourth, high correlation between incidents and complaints over time suggests that an in-depth qualitative analysis of complaints can provide important insights into passengers' (security) concerns.

This deliverable emphasizes the distinction between perceived and real security, as well as the difference between punitive and preventive security measures, though both of

these measures have the potential to improve or weaken perceived security. It is therefore crucial that security authorities and transport operators take into consideration not only the possible effects of proposed measures on actual security, but also asses its acceptance and perception by passengers.

Our analysis concludes that the effective explanation of security risks and security measures is the most important task of contemporary governments and stakeholders. In this process media plays a crucial role, both providing information as well as being a platform for the critical public debate of costs, benefits, and risks associated with existing and emerging security threats and issues.

1. Introduction

Decision makers in democratic societies must increasingly balance tensions between security and privacy while preserving citizens' trust. The recent revelations about far-reaching surveillance in many Western countries and the ensuing events demonstrate that more security does not always produce trust. This is because citizens' sense of satisfaction is not mere the absence of fear and the feeling of safety. Rather, satisfaction also requires a sense of freedom and the absence (be it real or perceived) of far-reaching security measures that infringe on privacy.

In addition to highlighting both the tension between security and freedom and the costs of security in terms of privacy, recent whistle-blower cases, namely those of Manning and Snowden, have also highlighted the role of the media in providing an outlet for whistle-blowers and as a watchdog of freedom, privacy, and civil liberties.

The dilemma of our times, for governments, for media, and for individual citizens, is thus the question of how much safety do we want and at what price. The answer to this question differs sharply according to the political orientation of the speaker. However, since the publication of Thomas Hobbes's Leviathan, it has been evident that safety and security, two essential features of the social contract, have their price. Freedom, both of the individual and of society, is a defining feature of legitimate government. Furthermore, governments are considered legitimate if they can resolve the tension between safety and freedom to the general satisfaction of the people [Hobbes 1651 (1960)]. In this process the media has come to play a critical role as a forum in which information is presented to the public, multiple claims and justifications are discussed, and essentially opinions can be formed.

In Leviathan [Hobbes 1651 (1960)], Thomas Hobbes made clear that danger and insecurity were always an essential part of human existence. The existential security in contemporary Western societies is unprecedented, yet the scale of the risks (in terms of their consequences), such as nuclear radiation, global warming, and terrorism, is also unparalleled. This is why security risks and safety are of such as large concern in today's societies and why they bring about such profound changes in the political order, shaping the perceptions, attitudes, and behaviour of citizens, politicians, and governments (Beck 2002; Inglehart 1997).

The differences, found among contemporary Western societies are caused by culture, as well as by the differences in national media. Hence, analysing media became crucial not only for understanding political communication, defined by Denton and Woodward as a "pure discussion about the allocation of public resources (revenues), official authority (who is given the power to make legal, legislative and executive decision), and official sanctions (what the state rewards or punishes)" (1990: 14); but also to understand which questions and topics play a dominant role in the political arena of contemporary Western societies.

This definition includes two key elements of political communication, verbal and written political rhetoric. However, going beyond this framework, according to McNair (2012), political communication also includes symbolic communication. These three elements of political communication will be covered in this report.

1.1 Politics in the age of mediation

Firstly, political communication includes all forms of communication undertaken by politicians and other political actors for the purpose of achieving specific objectives. Secondly, it includes communication addressed to these actors by non-politicians, such as voters and newspaper columnists. Finally, political communication also includes discussions about these actors and their activities in news reports, editorials, and other forms of political media (McNair 2012). For more on the interaction between media communication and policy research see D.6.3.

There are three principle groups of people between which the process of political communication is conceived and realized. The first is political actors. This includes political parties, public organizations, pressure groups, terrorist organizations, governments, etc. The second is media, and the third consists of citizens. Political organizations appeal to the media, seeking their assistance to convey their message through programs and advertising. In this the media serves as an agent of political organizations' public relations. But media then turns around and reports, comments, and analyses the actions of political organizations for citizens. Finally, citizens express their opinion through media – in polls, letters, blogs, citizen journalism, etc.

Terrorist organizations/acts of violence, even random violence directed against civilians, may be viewed as a form of political communication, intended to send a message to a particular constituency, and it is possible to identify and analyse such actions. The purpose of all political communication is to persuade; and the target of this persuasion – the audience - is the second key element in the political communication process. Without an audience no political message can have any relevance. Whatever the size and nature of the audience, all political communication is intended to affect the audience of the message.

In democratic political systems, media functions as a transmitter of political communication which originates outside media organizations themselves. But they are also a generator of political messages that are constructed by journalists and other producers, such as bloggers. Political actors must use the media in order to have their messages communicated to their desired audiences. Consequently, all political communicators must gain access to the media by some means. This access might be provided by law, such as when there are rules to ensure balance and impartiality in the media. Or this access could be engineered by political actors themselves, if they know how to draw the proper attention to themselves and gain airtime.

The media of course, does not simply report in a neutral and impartial way. Media accounts of political events are laden with value judgments, subjectivities, and biases. Political 'reality' comprises of three categories. The first is objective political reality, i.e. political events as they actually occur. The second, subjective reality is the ‘reality’ of political events as they are perceived by actors and citizens. The third, constructed reality refers to the events as they are covered by media and is critical to the subjective reality.

While arguments about the precise efficacy of the media continue, there is no disagreement about their central role in the political process, relaying and interpreting objective events in the political sphere, and facilitating subjective perceptions of them in the wider public sphere. For these media ‘biases’ are of great political importance - the extent and direction of media bias varies in a modern democracy, and its existence invites researchers to view media organizations as important actors in the political process and a subject of study.

Media is important to the political process in more direct ways as well. All newspapers take pride in their ‘public voice,’ i.e. the editorials in which they articulate political opinions. Sometimes these are presented as the voice of the reader, and directed at policy-makers. Alternatively, they may be constructed as the calm, authoritative voice of the editor viewing the political scene from a detached distance. In both cases, the editorial is intended as a political intervention, and is often read as such by a government or a party. And so the media is important in the political process also as transmitters of messages from citizens to their political leaders.

In their coverage of opinion polls, for example, the media may also claim to represent ‘public opinion,’ which becomes a real factor, key to understanding and evaluating a political situation, often in terms critical of individual politicians. With the use of the Internet, the media has extended its reach, both geographically and temporally, and as a result, the political arena is no longer confined to the domestic realm. Instead it has become more international and transnational, both in terms of political organisations and audiences.

In ‘ideal-type’ democratic societies, media communication fulfils the following five functions. First, media informs citizens of what is happening around them (the monitoring function of the media). Second, it educates the public about the meaning and significance of the ‘facts’ (the importance of this function explains the seriousness with which journalists protect their objectivity, since their value as educators presumes a professional detachment form the issues being analysed). Third, media provides a platform for public political discourse, facilitating the formation of ‘public opinion’ and feeding that opinion back to the public from whence it came. This must include the provision of space for the expression of dissent, without which the notion of democratic consensus would be meaningless. Fourth, media’s function is to shed light on governmental and political institutions, performing the ‘watchdog’ role of journalism. Fifth, the media in democratic societies also serves as a channel for the advocacy of political viewpoints. This function may be also viewed as persuasion (McNair 2011).

For the persuasion to be performed adequately, and thus the ‘public sphere’ to exist, a number of conditions have to be met. The political discourse circulated by the media must be: first, comprehensible to citizen; second, truthful in so far as it reflects the genuine and sincere intentions of speakers; third, means for transmitting information must be accessible to those who can be influenced by it; and fourth there must be institutional guarantee for the public sphere to exist. In short, democracy presumes an open state in which people are allowed to participate in decision-making, and are given access to the media, and other information networks through which advocacy occurs (Habermas 1996, McNair 2011).

Criticism of the media revolves around the question of manufactured consent. The legitimacy of liberal democratic government is founded on the consent of the governed, but consent, as Walter Lippmann observed, can be 'manufactured' (1946). This is defined as a 'self-conscious' art in which politicians combine the techniques of social psychology with the immense reach of mass media. The distinction between 'persuasion,' which is a universally recognized function of political actors in a democracy, and manipulation, which carries the negative connotation of propaganda and deceit, is not always an easy one to draw. The manipulation of opinion and concealment (or suppression) of inconvenient information are strategies that political actors pursue themselves, but with the help media institutions (McNair 2012). Further criticisms of media include the limitations of objectivity, the absence of choice, and the failure of education.

To summarize, the media is a crucial and multifaceted actor in the political process, fulfilling numerous vital roles. With the increasing globalization of media, political arenas have begun to transcend the boundaries of nation states and political communication has experienced profound changes. Comparative research can thus provide crucial insights into similarities and differences in communication patterns in these times of profound change in reporting and communication.

1.2 Structure of the deliverable

The first part of the deliverable offers a new theoretical framework for the comparative study of communication in the field of security.

The second part is an overview of the media landscape in the researched countries situated in both the national and international context. The global economic downturn of the past five years has hit the media sector particularly hard. The loss of financial sources has made news coverage more informative with fewer large investigative and analytical pieces, as they are more costly and require more staff. Journalists have been faced with unprecedented financial challenges, whereby they often had to compromise their journalistic ethics for commercial profit. However, trust of the media remains quite high, confirming our choice that media should be a subject of a comparative study of the dilemmas posed by balancing security and freedom.

In the third part, we define salience as a tool to study communication in the field of security.

The fourth and most important part of the deliverable, the analysis, studies salience as it relates to airports, critical infrastructure, and public transport. It highlights the need for new approaches to the communication of policy based on results from media analysis, ethnographic observations, statistical evidence, and semi-structured interviews with actors. These interviews with actors, namely policy-makers, stakeholders, and consumers, identified effective channels and patterns of communication about risk.

In the airport case study related media analysis concentrates on the media coverage and discourses related to 3D body scanners, as it is an issue which is directly related to airports and has potential relevance to the security versus privacy dilemma. The results indicate that airport authorities must consider the salience of security measures, and in particular the negative salience, in their consideration of the acquisition of security technology (along with the cost and benefit analysis) and training of security personnel. The training of security personnel, as well as effective communication with passengers, could increase passengers' positive responses to new security measures.

Stuxnet is not a technology that directly affects the daily life of common people. However, our analysis provides some important insights into the current nature of cyber security media reporting and debate. Cyber security is an important topic at the EU level, as well as at the level of individual member states. The media debate surrounding Stuxnet was very important, as it was the first transnational debate about cyber-attacks and cyber warfare. The media salience and resonance of Stuxnet also highlighted the degree to which cyber threats can affect the everyday activities of citizens.

To address the tension between security and privacy in public transport we have identified the use of CCTV cameras as a salient issue present in the media in most countries. The use of CCTV cameras is highly relevant for the Transports Metropolitans de Barcelona (TMB) and it was a dominant issue in the Spanish media. The issue is not controversial, and CCTV cameras are quite accepted by the majority of citizens as long as the data protection law is not infringed. Combining the analysis of the media coverage of security issues of two leading Spanish papers with the TMB security data and categorized complains data, the results of our analysis point to the following trends. First, economic issues prevail over security concerns due to the on-going financial crisis, though privacy remained a highly salient concern for Spanish citizens (specifically in regards to CCTV image data storage and sharing). Second, although security as a topic of concern has been supplanted by growing economic problems such as unemployment, the Spanish public is still very interested in maintaining its privacy.

In the fifth section we conclude both in general and in respect to the three case studies that it is crucial that security authorities and transport operators take into consideration not only the possible effect of proposed measures on actual security, but also asses its acceptance and perception by passengers. By acknowledging the distinction between actual and perceived security, as well as the difference between punitive and preventive security measures, both of these measures have the potential to improve or weaken perceived security.

In the sixth section recommendations are formulated. They emphasize that the effective communication of security risks and security measures is a critical task of contemporary governments and stakeholders. In this process media plays a crucial role in the dissemination of information, though it also provides a forum for critical public debate of the costs, benefits, and risks of existing and emerging security threats and issues.

2. Media landscape and social context in countries under study

The SECONOMICS media country reports clearly showed that one must be aware of existing ties between political actors and the media, as these ties have important implications for any media analysis (for more details, including a detailed description of the research design, see D.4.4 and its appendices 7,8, and 9). The diversity of our sample of countries, which included Central European (the Czech Republic, Slovakia, and Poland) and West European countries (Germany, Italy, Spain, and the United Kingdom), together with two overseas countries (the USA and Mexico),[1] allows us to observe some global trends, especially in terms of some major changes in ownership structures and regulatory frameworks.

The global economic downturn of the past five years has hit the media sector particularly hard. Profit margins are much lower than in the 1990s, several news outlets have been forced to lay off investigative and international journalists, reduce outputs, and limit the number of overseas branches. As Hronesova, Guasti, and Caulfield (2013) noted, “one of the strategies how to lower costs has become multi-skilling of staff and cutting specialist correspondents, foreign bureaux and investigative journalism, which has only reinforced the trend of journalistic *dumbing down*.” News coverage has focused on informative reporting rather than large investigative and analytical pieces, which are more costly and require a larger staff. Media content has also turned towards entertainment and tabloid-style news for commercial purposes. This has led to a negative trend in the media, referred to as “infotainment,” i.e. the presentation of news information in an entertaining and more appealing form (see Belakova 2013a). More importantly, media independence has suffered as outlets have increasingly depended on governments and large business to support themselves. Political and business interests leeched into media content, especially in countries worst hit by the crisis. On the positive side, the latest media developments have also seen a great diversification of news publishing and preference for online platforms due to their efficiency, accessibility and lower cost (Hronesova, Guasti, and Caulfield 2013).

While stressing these underlying factors and global pressures on the media sector, our comparative study highlights important regional similarities, especially in the three Central and Eastern European countries. While press freedom is highly ranked there (in the *Reporters without Borders* 2013 ranking, the Czech Republic performed the best out of all analyzed countries - see Table 1), the latest developments have seen the media

[1] Additionally, in the quantitative phase of the analysis Turkey was also included.

especially vulnerable to financial pressures through business and indirect political meddling. Since the beginning of 1990s, newspapers in the CEE[2] region have been mostly in the hands of large foreign media companies. However, as a consequence of the financial crunch, foreign investors in recent years left the region and the centralised media conglomerates were bought by local businessmen with diverse business interests (and political ambitions). This transfer of ownership often goes hand in hand with a change of editorial style (foreign owners rarely interfered with media content, but the local owners show a tendency to interfere with reporting). In addition, the fear of losing a job in very precarious times may also be driving self-censorship, but the degree to which it might be affecting content is difficult to judge (see Gawrecka 2013).

In terms of regulatory frameworks, the so-called Czech "Muzzle Law" of 2009 [3] undermined the constitutional right to inform and be informed and introduced strict limitations on freedom of speech. Only after severe criticism was the law amended in 2009 and today does not apply to cases of great public interest (such as political corruption). In Slovakia, the media have been negatively affected by politically motivated libel lawsuits and the distribution of state advertising (Belakova 2013a). As Belakova noted, "since by 2010 virtually every national daily had been involved in some libel case, media professionals felt that the threat of libel was shaping what was published" (Ibid.). In a similar fashion, the Polish media has been politically polarized since 1989, with occasional direct interference of major political actors, as documented by Sojka (2013).

Table 1: World Freedom of Press 2013

Country	Rating	World Rank
Czech Republic	10.17	16
Germany	10.24	17
Poland	13.11	22
Slovakia	13.25	23
United Kingdom	16.89	29
United States	18.22	32
Spain	20.50	36
Italy	26.11	57
Mexico	45.30	153

Sources: World Press Freedom 2013, Reporters without Borders

[2] Central and Eastern Europe (CEE) is here defined as the new EU Member States (2004, 2007, 2013 enlargement waves) and former communist countries of Eastern Europe.

[3] The so-called "Muzzle Law" Act 52/2009 Coll., amending Act No. 141/1961 Coll., introduced a ban on publishing any account from police wiretapping in newspapers, the Internet, TV, or radio.

As for the Western European countries, Italian media is certainly in the most precarious situation. De Gramatica's report clearly shows how media ownership in Italy directly determines what type of news can or cannot be published. Yet the situation is different than in Central Europe, as "the Italian media landscape breaks down into a myriad of partial, but not insignificant, holdings" (de Gramatica 2013, 10). Yet one actor dominates the Italian media sector, the former Prime Minister Silvio Berlusconi. Berlusconi's media empire has turned Italian public broadcasters into the extended arms of his political interests, which was apparent during every round of elections. The newspaper *Il Giornale* has been especially supportive of Berlusconi's *Forza Italia.* Due to these open political influences, Italian press freedom is usually assessed very poorly, which is reflected in all independent rankings.

The situation in Spain is to some extent similar. As Pereira-Puga and Hronesova (2013) noted, "although media freedom and independence has been respected in practice since the first democratic opening in 1975, the majority of media are economically dependent on the state and close ties with some political parties indirectly influence news reporting." Reporters without Borders have often criticized the ruling Popular Party for interfering in the appointment of editorial boards of the main Spanish media outlets. Similar to the Central European situation, Spain has also undergone some serious media ownership concentration, whereby the main media outlets are now in the hands of only a few holdings. Post-1975 democratic era Spanish newspapers such as *El Pais* retain a very good reputation, though, and despite their clear social democratic position are considered to be highly professional.

Germany and the United Kingdom present a different media landscape due to their long-standing journalistic traditions. Their media markets are also large and diverse, reaching beyond their borders. As Nitschke (2013) noted, Germany has over 300 dailies, 30 weeklies, and over 10,000 magazines, including one of the most respected weeklies in the world, *Der Spiegel*. The United Kingdom was a pioneer of journalism as we know it today. Britain was also the first country to develop a "public sphere where public opinion can be formed" (Hronesova 2013). Despite high journalistic standards in both countries, there are two caveats. First, due to the stricter security measures in the post-9/11 decade, both countries have adopted legislation curbing journalistic freedoms. In the UK, journalists are not only required to reveal sources and turn over material important for state security, but the 2006 Terrorism Act criminalizes speech inciting terrorist actions, a distinction which can be hard to make in some cases. Secondly, in Germany and the United Kingdom there are established links between high politics and media owners and executives, which occasionally translate into influence on news coverage.

The British case is also interesting for the unique self- regulatory nature of the British press. The analysis in the British national report shows that until recently an independent commission oversaw the media in the UK. However, following the 2011 phone-hacking scandal at the weekly *News of the World,* the British government launched a public inquiry into the general regulatory framework, which is currently undergoing major reforms. The scandal in fact uncovered an important flaw in British media ownership regulations, as private media outlets have come into hands of a handful of companies with political interests. Each main daily has a somewhat different ownership structure, whereby *The Guardian* has the most transparent one. The management of the newspaper is answerable only to its owners (Scott Trust Ltd.), and conducts and external annual audit. The newspaper also has an independent Ombudsman, who is in charge of complaints.

Unlike the direct influence in Italy and Spain, US media has been assessed as one of the most politically independent and most commercial in the world (Belakova 2013b). Media freedom is one of the anchors of the US constitutional system and the courts have in the past often ensured that they are protected from libel and defamation suits from public figures. As the press is predominantly in the hands of private companies, the news sector is driven by commercial interests. This also leads to only a limited diversity of news as the focus is on newswire reports. The financial crunch had a serious negative impact on investigative journalism in a similar fashion as elsewhere. However, it has also led to a change of ownership structures. Previously, individual owners (mostly influential families) owned important news outlets. In the aftermath of the financial downfall, though, large corporations and tycoons have started to bail out media outlets in financial difficulties. Most notably, Amazon founder Jeff Bozos bought the Washington Post in 2013.

Lastly, in Mexico the position of media is dramatically different. Mexico is a dangerous place to be a journalist. Due to the on-going war between the state and drug barons, tens of journalists get killed every year. Moreover, political censorship is omnipresent. It was especially strong during the controversial July 2012 elections, which brought the Institutional Revolutionary Party back to power (Vamberova 2013). Citing the Reporters without Borders 2013 report, Vamberova highlights the low level of journalistic freedoms, as well as threats journalists are facing. “They are threatened and murdered by organized crime or corrupt officials with impunity. The resulting climate of fear leads to self-censorship and undermines freedom of information” (Vamberova 2013: 9). In terms of quality of the press, Mexico is dominated by the so called red press, i.e. “news focusing on assassinations, kidnappings, and drug crimes” (Ibid.). Mexico also faces a high concentration of media ownership in the hands of only a few influential businessmen, such as Mario Vázquez Raña.

The global economic malaise of the past few years has had a clearly negative impact on the media sector in the studied countries. Ownership has slowly shifted into the hands of fewer and fewer businessmen and tycoons, and ownership restrictions have relaxed limits on market shares (with the exception of the UK).The quality of the produced news and analyses has also suffered under financial constraints. Journalists have been faced with unprecedented financial challenges, whereby they often had to compromise their journalistic ethics for commercial profit.

In addition, there has been a trend of political meddling into editorial policies and news content as media owners often have close ties to important political actors. There is a clear difference in terms of freedom of the press and the quality of journalism across the studied countries, though. While Central European media score highly in terms of media freedoms, the quality of news reporting is much lower, and informative, rather than analytical pieces, dominate.

On the other hand, both the United Kingdom and the United States provide investigative and analytical news reporting at highest professional journalistic standards. Italy and Spain struggle with the influence of big business and politics over media content, but still offer diversified and quality journalistic reporting. Lastly, Mexico is a clear outlier in the set of analyzed countries and was even assessed as the most dangerous country for journalists on both American continents, mainly due to the on-going cartel wars (Reporters without Borders 2013).

2.1. The Domestic and International Context

In recent years, security threats such as terrorist attacks, global organized crime, and cyber-attacks have come to the forefront of the world attention, creating new settings for worldwide security challenges. As analysed in the *SECONOMICS* country reports (see D.4.4., appendices 7, 8, and 9 for summaries, and the project website for full text reports), the 21st century is facing post-modern challenges and risks, risks that develop from the latest technology, opening new, virtual opportunities for crime. Terrorist attacks, intelligence leaks, and direct or indirect participation in global or national cyber-attacks have significantly influenced the latest policy priorities in the field of national security. The protracted financial crisis has further intensified concerns for public safety as crime is expected to grow during times of economic malaise.

These developments have been reflected in the national security concerns and strategies[4] of all studied countries, which have reacted by adopting new security measures and laws. Within the studied period of 2013, a series of high-profile cases concerning leaks of top-secret intelligence data have raised questions about the legality of security practices used by national governments. These eye-opening revelations have intensified debates about which powers national intelligence services can reasonably wield over the public. Whistle-blowers, such as Chelsea Manning, Edward Snowden, and Wikileaks founder Julian Assange, have come to symbolize the controversy surrounding these state programs and questions about the appropriateness of secretive state intrusions into the private lives of their citizens, intrusions which are usually justified by the War on Terror and carried out under the aegis of counter-terrorism. As indicated in the individual country reports, negative perceptions of security and the question of who controls the controllers have gone hand in hand with debates about the need for increased protection against global crime.

In view of these global events, and taking into account domestic political and economic developments, each of the studied countries has prioritized a specific aspect of its national security. Countries that are generally more active on the international scene,

[4] Of the studied countries, Italy alone has no clear security strategy (de Gramatica 2013).

or have had a previous experience with domestic and international terrorism, are generally more exposed to (and hence concerned about) potential terrorist attacks. Such countries (the UK, the US, Spain, and Germany) prioritized airport security in the form of body scanners and intensified CCTV camera coverage (Nitschke 2013). Surveillance and improved transportation security measures have been top government priorities, especially since the 9/11 attacks in New York City and the 7/7 2005 attacks in London. The current trend towards installing more surveillance systems and scanning devices in public spaces has often included invasive security devices, such as the 3D body scanners, at the cost of intrusions into privacy. Countries dealing with large-scale organized crime, such as Mexico, which finds itself in the midst of a drug war, have also been strengthening their surveillance capacities (Vamberova 2013).

On the other hand, in countries with no real danger of a terrorist attack by international extremist groups, there is little policy interest in advanced and costly security devices, such as full body scanners. Although some countries in Central Europe, such as Poland and the Czech Republic, have become part of the global war on terror by contributing their soldiers to military actions, the governments of those countries believe that the risk of terrorist attack is very low (see Sojka 2013). Nonetheless, surveillance is also very topical for reasons of improving overall public safety – especially in capitals and transportation hubs. Though for different reasons, concerns for national and public security have thus in the studied period ran very high in all studied countries.

After the widely covered terrorist attacks of the last two decades, a series of new policy approaches have been introduced which fall within the scope of the three studied topics of this project. The 9/11 terrorist attacks in New York, and especially the Christmas Day 2009 bomb attempt on a Northwest Airlines flight, have shaped US security policies significantly. As Belakova (2013b) noted, the failure of US intelligence to act pre-emptively during the 2009 bomb attempt "triggered a fierce discussion among lawmakers, authorities, experts, and advocacy groups about air travel security measures." In Europe, the 2004 Madrid train bombing and the 7 July 2005 attack in central London provided evidence that, after 9/11, terrorism is a global issue, rather than the domestic issue it had been in the past in countries such as the UK (IRA) and Spain (ETA). As such, it merits global strategies and approaches (Pereira-Puga and Hronesova 2013). As documented in the report by Nitschke (2013), Germany has successfully prevented at least seven terrorist attempts in the past decade. Italy experienced its last terrorist attempt in 2003, but the death of Italian soldiers in a bomb attack in 2010 in Afghanistan (de Gramatica 2013) gave weight to the voices arguing for new security technologies.

These terrorist attacks and attempts across the studied countries in Western Europe and overseas have intensified calls for a transnational counter-terrorism strategy. In fact, cooperation in the field of transport and airport security has increased. The US Department of Homeland Security and the Transportation Security Administration developed the so-called multi-layered approach to security. This includes the "increased sharing of intelligence and boarding pass information, the widespread use of body scanners, officers monitoring human behaviour [sic] in airports and closer relationships with airport officials around the world" (Belakova 2013b). Anti-terrorism databases have been created in Germany and other countries which share information about the principle terrorist groups around the world (Nitschke 2013). In the UK as well as in the US, the already discussed full body scanners were introduced at airports (Hronesova, Guasti, and Caulfield 2013). The scanners were believed to improve security in aviation by detecting liquids and non-metallic objects. However, some religious and human rights groups challenged their introduction since the scanners virtually stripped passengers naked. Their invasive nature and the consequences for human dignity and intimacy of the scanners (see Nitschke 2013), as well as their potential health hazards, were discussed by the European Parliament in 2010. So far, neither a global nor a European position on the application of these devices has been adopted.

Furthermore, the installation of monitoring devices has significantly increased in the last two decades. In the US, the number of CCTV cameras had increased by approximately 30 million from 2001 to 2011 (Belakova 2013b). Out of all the studied countries, Great Britain has the highest number of closed-circuit television cameras per person. According to the British Security Industry Authority, 5.9 million CCTVs have been installed in the country since the 1980s (Hronesova, Guasti, and Caulfield 2013). Similarly to the body scanners, the most discussed topic in debates about CCTV has been their intrusive nature and their potential to violate privacy rights. Such debates were most prominent in the US and the UK, but they have often been ignored, given CCTV's alleged benefits. For the sake of greater public safety, stricter security measures have been generally accepted by the public. As reported in the UK national report, "from the initial outrage at living in 'one nation under CCTV,' watched by the Orwellian 'Big Brother,' CCTV has become a point of ridicule, mockery and humour" (Hronesova, Guasti, and Caulfield 2013). Similarly, as shown by Sojka (2013) in the post-communist part of Europe, "CCTV cameras have become in a very short time a social status symbol and constitute an inseparable part of the post-1989 modernization processes." In the Slovakian case, Belakova (2013a) argues that the relatively high frequency of private surveillance was due to the fact that CCTV cameras in private homes have become trendy in the country and a sign of a social status.

The main argument in favour of CCTV over the past two decades has indeed been the decreasing crime rate around the world, a decrease that has occurred despite the continuing economic malaise. CCTV footage has generally been used to solve crimes, but also to deter crime. As Belakova noted, "technological advancements, including surveillance equipment such as CCTV cameras, were thought by some to have contributed to the downward trend in crimes statistics" (Belakova 2013b:25). However, not all analysts agree with this assessment. They argue that decreasing crime rates are a product of socio-demographic changes, rather than an effect of policy, i.e. CCTV (see Hronesova, Guasti, and Caulfield 2013). Although the link between increased surveillance and lower crime rates worldwide has still not been confirmed (see Belakova 2013b and Hronesova, Guasti, and Caulfield 2013), it is clear that CCTV cameras can be used as a good mechanism for solving crimes and identifying perpetrators. Immediately after to the studied period, on 15 April 2013, an improvised bomb exploded by the finishing line of the Boston Marathon, killing 13 people and injuring over 260.

Surveillance footage as well as private videos from smartphones were used during the following successful manhunt of the suspects. In this respect, surveillance footage can rapidly increase the time it takes to solve a crime and find the perpetrators (see Pereira-Puga and Hronesova 2013).

Recently, cyber-crime has become a typical high-volume crime in the UK which often outnumbers burglary and robbery cases (Hronesova, Guasti, and Caulfield 2013). Cyber-crime uses information systems and technology to commit extortion, identity theft, espionage, or even paralyse critical infrastructure. As analyzed in this project, in June 2010 a worm was developed by the USA and Israel to interfere with uranium enrichment in the Iranian nuclear facility at Natanz, which opened a new era of cyber war. Stuxnet was designed as a highly sophisticated piece of malware which targeted a very particular section of the Iranian nuclear facility. The reason why Stuxnet has shaken the public views about cyber security is that it was unprecedented in its scope and effectiveness. As a highly sophisticated weapon, it was able to penetrate the Iranian nuclear facility in a quasi-autonomous fashion (see Belakova 2013b). However, Stuxnet has been only one among many recent cyber-attacks, though it has certainly been the most destructive one so far. In response to these developments, the British Government released the National Security Strategy and the Strategic Defence and Security Review in October 2010 and devoted over £650 million to increase cyber security (Hronesova, Guasti, and Caulfield 2013). Also, in the US network intrusions were reportedly widely considered to be one of the most serious potential national security challenges in 2012. In response, Congress passed the Cyber Intelligence Sharing and Protection Act in an effort to protect private computers (see Belakova 2013b).

Furthermore, the global threat of terrorist attacks and cybercrime has also prompted the passage of new laws. This trend was especially strong in the United Kingdom and the United States. The British Terrorism Act of 2006, Counter-Terrorism Act of 2008, and Terrorism Prevention and Investigation Measures Act of 2011 introduced strict measures and zero tolerance towards any extremist views which could potentially lead to violent terrorist acts (Hronesova, Guasti, and Caulfield 2013). Even countries that are less likely to be the victim of a terrorist attack have adopted new measures. Although “terrorism does not represent a threat to the population” in Italy, the government adopted new anti-terrorism legislation in 2005 (de Gramatica 2013). Stricter laws have inspired a counter-trend in regulating the intrusive nature of monitoring systems, which have recently begun to be more regulated in some countries such as Slovakia and Spain (see Belakova 2013a and Pereira-Puga and Hronesova 2013). In all European countries under study, CCTV footage is strictly limited and may be kept only for a certain period of time and is to be used only for the purposes of criminal investigation. The weak rule-of-law in Mexico, though, allows for the misuse of footage (Vamberovay 2013). The legal repercussions of the new security risks have thus combined both increasingly stricter laws with a growing concern for the arbitrariness of state intrusions into privacy.

In 2013, the countries under study have been influenced both by domestic political developments and domestic crime, as well as international political developments, especially related to the on-going military actions in Afghanistan and Iraq. In the aftermath of reoccurring terrorist attacks, law-enforcement authorities and politicians periodically called for the introduction of more advanced surveillance technologies, including face recognition and full body images. Even in countries with lower exposure to terrorism, concerns about increasing crime rates during the economic crisis, as well as the global emergence of cybercrime, have inspired stricter security measures. It can be expected that post-modern security risks will only intensify with advancing modern technologies. As a consequence, a growing concern for the respect of privacy and intimacy – both physically and online – will require an adequate legal response from individual states.

2.2. Trust in media and information sources

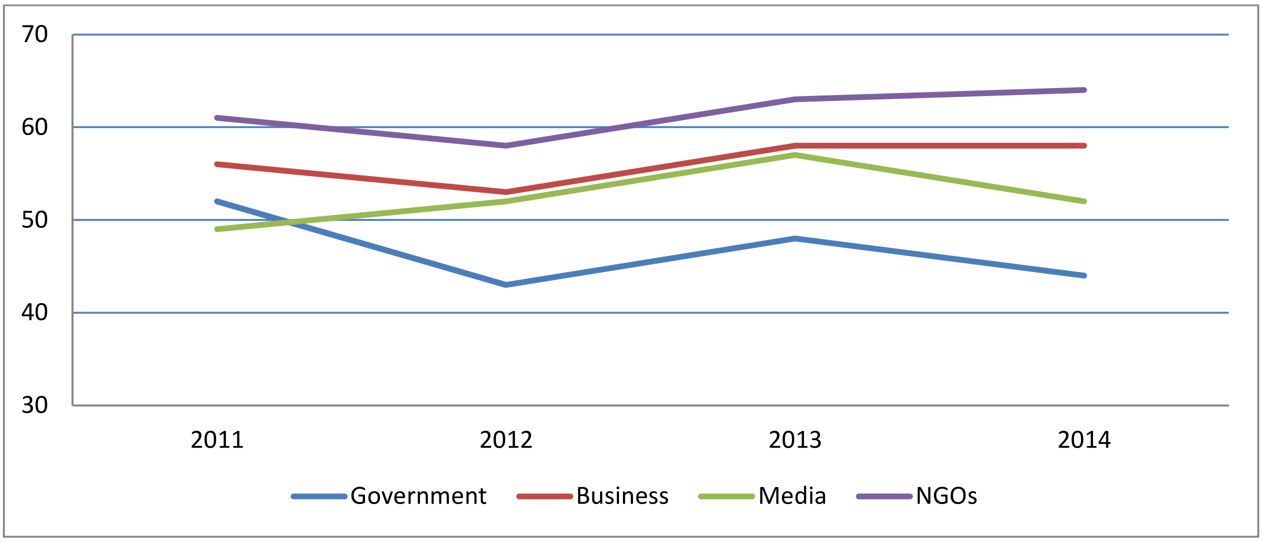
Analyzing the media as a communication channel offers a good basis for understanding the communication patterns between policy makers, stakeholders, and citizens in the areas of security and risk. Furthermore, the communication channels and patterns are currently under-researched, and the media offers a good basis a for comparative analysis of the topic. The identification of effective channels and patterns of communication and risk prevention for relevant target groups will thus provide an important scientific and practical contribution to the field.

In order to further prove that the media is the proper lens through which to help us understand communication, we present an analysis of public trust in media in comparison to other actors.

However, the secondary analysis of empirical data from international surveys such as Eurobarometer, the European Social Survey (ESS), and others offers only limited knowledge about a limited number of European countries over a limited time period.[5] In order to include the most recent secondary data for the countries under study, Figure 1, with the Edelman Trust Barometer[6] provides a comparison of more than twenty-five countries between 2011, 2012, and 2013 comparing not only trust in institutions (as the Eurobarometer does), but also attitudes towards business, government, NGOs, and the media.

[5] Eurobarometer surveys provide information on trust in government and various state institutions as well as the press, radio, internet, and NGOs regularly. Data from 2003-2012 was analyzed and is available online at http://ec.europa.eu/public_opinion/index_en.htm [last visited 7.3.2014].

[6] Edelman Trust Barometer survey was produced by research firm StrategyOne and consisted of 20-minute online interviews. For 2012 ETB the online survey sampled 25,000 general population respondents with an oversample of 5,600 informed publics in two age groups (25-34 and 35-64) across 25 countries. All informed publics met the following criteria: college-educated; household income in the top quartile for their age in their country; read or watch business / news media at least several times a week; follow public policy issues in the news at least several times a week. For 2013 ETB, more than 31,000 respondents in 26 markets around the world were surveyed and their trust in institutions, industries and leaders was measured. Available online http://trust.edelman.com/ [last visited 7.3.2014].

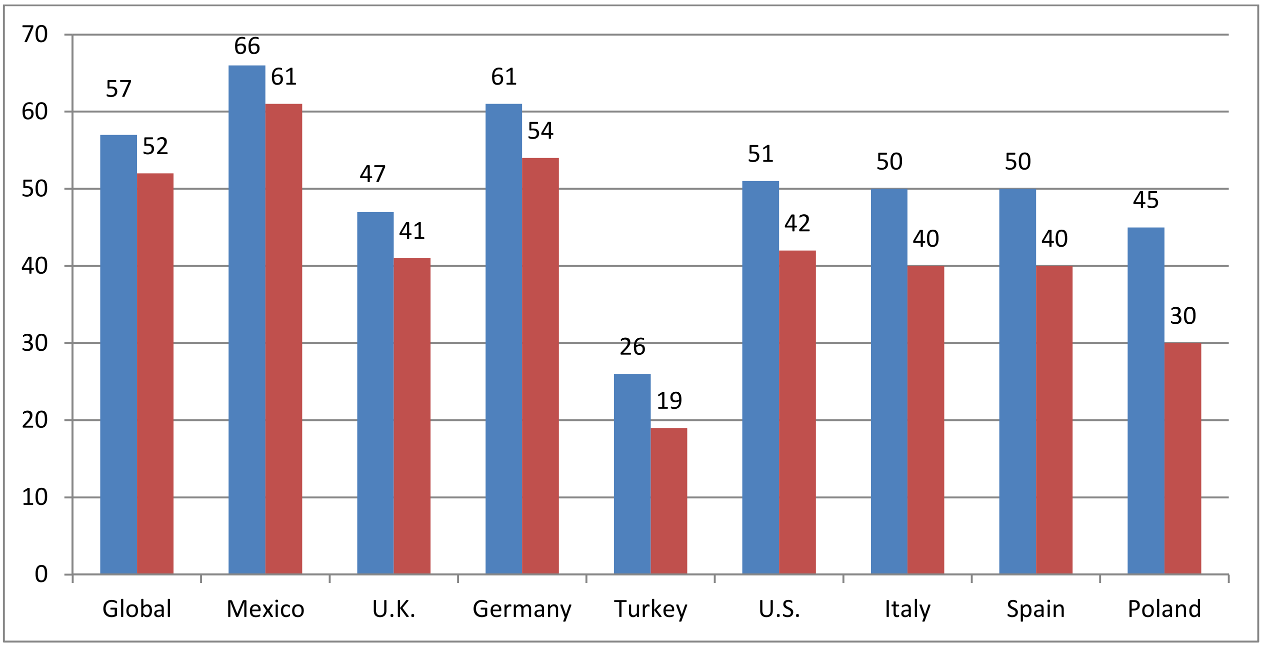


Source: Edelman Trust Barometer

Figure 1: Trust in institutions (in per cent)

Comparing the trust in these four institutions in 2011, 2012, 2013, and 2014 (older data is not available) in Figure 1, we can see that trust in media is quite high, reaching its peak in 2013 and decreasing slightly in 2014. We also see that while the trust in business and NGOs is higher and shows a similar pattern, the trust in the media is since 2013 showing similar pattern as trust to government (although trust to media is consistently higher than the trust in government (by ten percentage points). We can find different explanations for this in the literature (Berry 2013; Kiousis 2001). While media is trusted, the change we see, and especially the slight decrease in 2014, can be attributed to the profound change in media structure, ownership, and performance and the shift from traditional printed media to online news, social media, citizens reporting, etc. While traditional media sources are still highly trusted, the diversification of media continues.

Trust in the media varies across countries and is significantly influenced by age, education, and social standing. Figure 2 shows that trust is generally higher in emerging and developing countries than in developed countries. The figure also shows both the variation and the decrease in trust in media in countries included in the SECONOMICS sample. The biggest outliers are Turkey, the UK, and Poland. Turkey is a specific case, where deep divisions in Turkish society are also reflected in media trust. In the UK and Poland, the trust in media was, among other factors, negatively influenced by (recent) scandals, including public probes into media reporting, such the Rywin Affair in Poland from 2002 to 2004, and the Levenson Inquiry in the UK from 2011 to 2012.



Note: The blue column is 2013 and the red column is 2014. Only countries included in the SECONOMICS sample are visualised.
Source: Edelman Trust Barometer[7]

Figure 2: Trust in media: Comparison of 2013 and 2014 (in per cent)

The analysis of the secondary data on trust in the media confirms the appropriateness of our choice of media as a platform for the comparative study of the dilemma between security and freedom. Furthermore, the SECONOMICS case studies will not only provide new and unique perspectives, but also strengthen the overall cohesion of the project.

[7] http://www.edelman.com/insights/intellectual-property/2014-edelman-trust-barometer/about-trust/global-results/ [last visited 16.2.2014]

3. Defining Salience and Media Communication

Salience is a term in public opinion, communication, and policy research which originally developed in semiotics and referred to the relative prominence of a sign. In communication research salience refers to the accessibility of frames and narratives, which are the narrative structures in which information is presented, in (mass) communication. For the purpose of this study, salience is defined as the public perception and acceptance of security issues, and more particularly of security measures. For these purposes salience signifies the degree of acceptance (positive salience) and the degree of rejection (negative salience) of security measures.

We distinguish between media salience as a proxy for potential acceptance or refusal of security measures. The key aspects of salience, such as its direction (positive/negative) were measured in the comparative media analysis, and amended by data from the customer surveys (airport, public transport) and customer complaints (public transport). Our extensive research highlights low to medium salience (predominantly positive) as the main condition for successful communication and acceptance of security measure.

Our main task was to conceptualise security and risk as a social phenomenon and analyse their mutual interplay in public opinion and attitudes, and to then identify policy interactions between policy makers, industry (stakeholders), and citizens (consumers). We have used the method of comparative qualitative analysis as a tool for obtaining and studying qualitative data for comparative analysis of risk and security related discourses and patterns of communication. This tool not only enabled us to identify effective channels and patterns of communication and risk prevention for relevant target groups, but also generated a unique corpus of comparative data on nine countries over a period of forty months.

All articles were selected from a period between January 2010 and April 2013, from two of the most circulated quality dailies in the following countries: the old and the new EU member states of the Czech Republic, Germany, Italy, Poland, Slovakia, Spain, and the UK, as well as non-EU member states, the USA, Turkey, and Mexico. The twenty national newspapers contained over 2800 relevant articles in the given period, while expert blogs contributing approximately 400 additional articles. In all countries one left-wing and one right-wing media outlet was selected. In the Spanish case one national and one Catalonian daily were selected in order to allow closer interaction between the media analysis findings and the case study on public transportation (Barcelona). The interim product of the analysis is a corpus of almost 3200 articles related to the issues of 3D body scanners, Stuxnet, and CCTV camera systems.

The focus of the SECONOMICS project is on the definition and perception of risk and security in three different settings: airport security and air travel, critical infrastructure, and urban transport. The findings of our qualitative comparative analysis of media perception of terrorism threats and security measures suggest that the way media portrays different security risks depends on several factors. Past experience with a particular security threat, as well as the probability of the country being targeted in the future, account for the main differences in the extent of coverage dedicated to the issue in the domestic media.

In terms of evaluative frames, the nature of the security risk as well as of the technological measure (3D body scanners, CCTV cameras, Stuxnet) plays a role in the framing of the topics. Technologies that are considered intrusive (e.g. 3D body scanners), receive more negative coverage than less intrusive technologies (e.g. metal detectors), even if the particular risk the security measure tries to mitigate is considered high. In those cases, less intrusive technological measures are deemed preferable by the media and, by implication, the public, as potential terrorist threats are not perceived as satisfactory tradeoffs against imminent health risks. Thus, security measures themselves may become seen as producing new, unnecessary risks and evaluated negatively in the media and by the public.

In political communication there is a trend that terrorist threats are generally first presented before arguments for security measures are made. This is especially true in discussions of 3D body scanners and CCTV systems. Stuxnet does not follow this pattern so strictly, as it is in part presented as a security measure against the potential Iranian nuclear threat, and in part as a cyber-terrorist threat. In the Central and Eastern Europe, terrorism and terrorist threats are presented as external, international issues, which have little relevance to local citizens, as terrorist attacks in these countries are unlikely (this includes the Czech Republic, Slovakia, and, to a lesser degree, Poland).

Within this trend, the coverage is dominated by the actions and opinions of different foreign states, state institutions, and politicians who discuss the merits of introducing security measures and the related rules and regulations which safeguard against intrusions into citizens' privacy and potential health risks. Health, privacy, and dignity concerns prevail over security risks (which are seen as not great). In countries where the analytical quality of the media is higher (Germany, the UK) other tradeoffs such as costs vs. effectiveness and privacy/freedom vs. security are discussed.

With regards to the volume of coverage, the Stuxnet attacks were in the middle. The issue was presented as foreign or technology news. In most countries, with the exception of Mexico, the analyzed articles were mostly informative. As a general rule, the coverage followed international developments and information revealed by foreign newspapers (from the US and UK). The overall message of the Stuxnet debate focused on three types of security risks. Firstly, the extensive scope of Iran's nuclear programme was a justification for the attack and may indicate that the media believed there is a real possibility of a future threat to the Western world's security in the form of Iran's development of a nuclear weapon. Second was the deployment of new technologies in state cyber warfare. Thirdly was the coverage that indirectly suggested the potential risk of a nuclear or other environmental catastrophe, similar to Chernobyl (1986) or Fukushima (2011), if more modern technologies are deployed in state cyber-attacks.

The use of CCTV cameras was the most salient topic in countries where the probability of terrorist attacks is considered low. The coverage was framed mainly in terms of the actions and opinions of municipalities, journalists, school authorities, and citizens in relation to the use and installation of CCTV camera systems. The evaluation of the merits of CCTV cameras and acceptance of their introduction depended primarily on the space that was being monitored, and did not change much over time. CCTV cameras were very often framed in terms of effective crime prevention, detection, and solution, and as such accepted in countries were crime is considered a high risk (e.g. Mexico – drug-related crimes, Spain- ETA terrorist threat).

The second trend, particularly true in Italy, is usually present in countries where the security threat is perceived as imminent and the media debate is dominated by politicians. In this case, the urgent need for solutions is overemphasized in order to limit (or avoid) time for reflection. The motivations driving political actors' often emotional appeal to citizens' inherent fears, such as those of the *Lega Nord* party, is political saliency of the issues and possible electoral gain. Unlike in the first trend, where terrorism is something external and not immediately threatening citizens of the country, in the second trend, the world is portrayed as full of global risks, to which only modern technology, presented as an efficient solution, can provide answers. In this over-simplified portrayal of reality, the facts are less important than emotional appeals, and renouncing privacy and intimacy for security is portrayed as a necessity.

The coverage of Stuxnet in Mexico can be seen as falling into the second trend, as unlike any other country in the sample, Mexican media clearly side with Iran, denounce the attackers (identified as the USA), and highlight Iran's right to sovereignty. In an interesting twist which can be explained by the complexity of the US-Mexican relations, Mexico sees itself as a possible target of similar attacks in the future.

Another good example is the coverage of CCTV cameras in Poland, where we observe an emerging debate about the need for a comprehensive law which would regulate the use of public and private monitoring systems. However, the debate is not framed in terms of transportation security, but rather in terms of how CCTV is used to detect, prevent, and solve crimes. In some cases this project's national reports link some countries' less critical and less complex understanding of CCTV with their post-authoritarian development (namely Poland, Spain, and Italy). However, this trend is quite opposite in Germany, where the past experience with a totalitarian regime heightens the sensitivity to the trade-offs between security and privacy, human dignity and freedom.

4. Analysis

The following analysis represents a new and innovative approach to policy communication based on connecting findings from media analysis, ethnographic observations, statistical evidence and semi-structured interviews with actors, i.e. policy-makers, stakeholders, and consumers. The aim is to identify effective channels and patterns of communication and risk.

First, the airport case study focuses on the relationship between the acceptance of security measures and security perceptions of passengers (i.e. customers). In airports there is a high density of people located in a particular area, which translates to a potentially high death rate in an attack. Furthermore, the passengers' cultural and ethnic background varies, and so does their sensitivity to security measures, as these are closely related to their perception of freedom and privacy, discrimination, as well as sensitivity to possible threats. In the airport case study, related media analysis concentrates on the media coverage and discourses related to 3D body scanners as an issue which is directly related to airports and is potentially salient in the security versus privacy dilemma.

Second, the case of critical infrastructure, represented in the SECONOMICS project by the UK energy company, National Grid, differs from air and public transport. In respect to critical infrastructure, the end user is not an individual (a consumer or passenger, as in the previous case), but the transmission network and its stakeholders. Of course critical infrastructure concerns citizens in very profound way. However, this effect is indirect, and often difficult for citizens to comprehend. One of the biggest challenges in the study of citizens' perception of security measures was selecting an issue which relates as close as possible to critical infrastructure, yet would be transnational and thus possible to study using comparative media analysis. Stuxnet was selected as a topic for analysis as it affects critical infrastructure, cyber security, and as the course of Stuxnet's evolution is also an example of a security measure turned security threat (for more on cyber threats and the security of large scale IT networks see also D2.3.).

The third case study, which relies on cooperation with TMB, combines data describing the salience of security measures taken from our media analysis, with the TMB's passenger complaints, as well as further information that introduces a critical salience index of security measures. This enables the research team to address the distinction between actual and perceived security, as well as the difference between punitive and preventive security. In the interaction between the media salience data and the case study data from industry partners, we find that it is crucial for transport operators to consider not only the possible effects of proposed measures on actual security, but also asses its acceptance and perception by passengers.

4.1. Air transport and 3D body scanners

In the airport, passengers are rather unlikely to be fully aware of the complexity of the airport and of the airspace (and thus unable to grasp the security measures concerning the airspace organization and airside- and landside-based measures). We can thus with high certainty predict that passengers will be concerned with privacy and comfort rather than with the feeling of safety. The regular monitoring of service performance and customer satisfaction supports this assumption[8] (Carta 2012).

In the airport case study, the media analysis concentrates on the media coverage and discourses related to 3D body scanners as an issue which is directly related to airports and has a potential for salience in the security versus privacy dilemma.

The introduction of 3D body scanners to increase security at airports has been a very important and frequently debated issue in recent years, both at an institutional level, as well as at a societal level through media and public debates.

Backscatter X-rays and millimeter wave scanners are competing body imaging technologies that are used to perform full-body scans of passengers to detect hidden weapons, tools, liquids, narcotics, currency, and other contraband materials. These innovative security technologies are also referred to as "3D body scanner," "whole body imager (WBI)" and "security scanner" (from the EU commission in its official reports and regulations). The implementation of widespread full-body scanners has generated public controversy, since both full-body scanning technologies allow security screeners to see the nude surface of the skin under clothing.

Some claim this very invasive ‘total body’ screening violates basic human rights. It does not respect physical integrity and personal dignity, as well as privacy and data protection rights. Moreover, many concerns have been raised with respect to its potential negative impact on health and on its usage on children. In addition, its efficacy and efficiency have not been completely proven, since a high error rate has been reported and the scanning time seems to be also higher than other security screening measures. Besides 3D body scanners there is other security equipment, such as CCTV equipment, biometric readers, etc.

Capital expenditure in security related activities has risen sharply due to new security standards in the aftermath of 11 September 2001 as well as the mandated requirements and timescales in Regulation (EC) No 2320/2002, particularly those related to the screening of checked baggage. These have required some airports to significantly increase investment in security equipment and facilities (D1.3, version 0.1, p. 12). From the point of view of security/privacy it is interesting how new measures are spoken of and justified by policy makers and stakeholders to passengers. “Before screening, coats and jackets of passengers shall be taken off and shall be screened as cabin baggage. Passengers shall be screened by hand search or WTMD [walk-through metal detector]

[8] In the 2012 Carta survey, - 93% passengers show a high level of satisfaction with bag control service (security perception) and the same proportion of passengers are satisfied with personal safety/security, thus underlining the security versus service duality (Carta 2012).

equipment. Where the screener cannot determine whether or not the passenger is carrying prohibited articles, the passenger shall be denied access to security restricted areas or rescreened to the screener's satisfaction" (D1.3). The communication strategy as well as the implementation of security procedures has an important effect on how the security measures are accepted and how they influence customer satisfaction.

4.1.1. Media analysis and security measures

The debate about 3D body scanners in the analyzed countries (for more detail see D4.4 and its appendices) was dominated and led by the media, with the media in other countries mostly reacting to events in the US and bringing their own agenda and domestic context into the debates. Among the European countries there was not much evolution of opinions over time. The UK, Netherlands, and Italy are supporters of 3D body scanner technology. The rest of the analyzed countries are rather critical. The general attitudes towards 3D body scanners among various actors are similar in all countries. The most important actors in the debate are transport security agencies, state institutions, and politicians. While transport security agencies and politicians are strong proponents of 3D body scanners, the attitudes of passengers, advocacy groups and experts towards the adoption of this measure are rather mixed, leaning towards critical. The outlier in this general trend is Italy, where in a debate dominated by political actors, the passengers seem to be strongly in favor of the adoption of the 3D body scanners.

Generally we can say that the number and diversification of actors involved in this issue increases over time as more groups join the discussion. The dynamic of the whole debate is also interesting. Almost all of the articles were published in a relatively short period after the discussion had started and then the topic left the discourse again. The curve of public support for the installation of the security measures would follow the same trend as the level of perceived threats, increasing rapidly after an accident or attack, but it tends to wane as quickly as it appear (Mansfeldová and Guasti 2013).

The biggest distribution among the actors could be found in the US. As the 3D body scanners are primarily a topic in the US, the majority of actors coded there were domestic ones. In the other countries international actors dominated in the debate.

The passengers' arguments against 3D body scanners and their critique have different reasons. The most important points of criticism are privacy, health, and quality of service. The media also focused on cultural differences when defining privacy because sensitivity to security procedures and regulations can be influenced by passengers' religious, ethical, and ethnic background (Mansfeldová and Guasti 2013). The health argument centred on the potential risk of cancer caused by radiation released during the process of scanning. Besides the health risk and privacy arguments, respondents also mentioned insufficient quality of service.[9]

The first two critical points – privacy and health – require better communication with citizens using all communication means. The opinion of passengers concerning the quality of service differs (see D4.4), [10] however it is an important finding for stakeholders, who can consider the importance of strengthening communication skills in personnel training in order to positively influence customer satisfaction.

4.1.2. Case study of salience of security measures: Acceptance of airport security

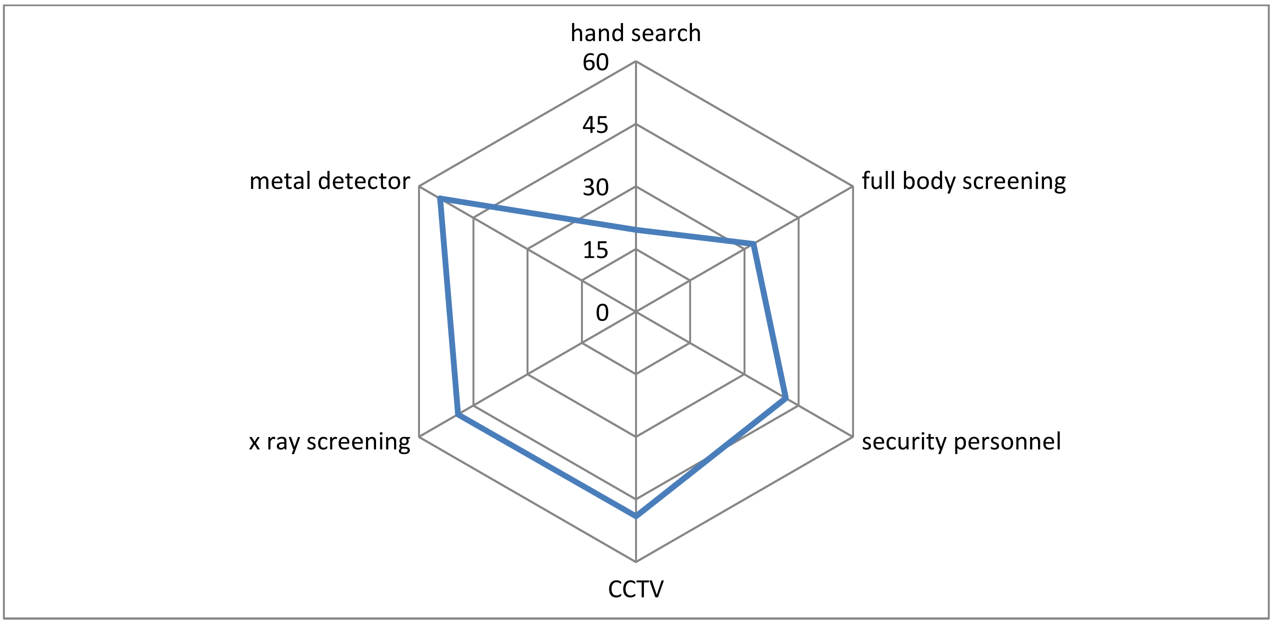
Unlike in the case of the Barcelona metro, where passenger data (provided by TMB and expanded upon jointly by TMB and The Institute of Sociology of the Academy of Sciences of the Czech Republic (IS AS CR) to demonstrate the role which social acceptance plays in the successful implementation of security measures) was available to analyse the salience of selected security measures, no such data is available for the airport case. Instead the team at Anadolu University prepared and collected passenger surveys (January 2013, sample of 904 passengers, of 82 nationalities at the International Terminal of Ataturk Airport in Istanbul).[11] This data, although neither systematic nor large-scale, offers a unique and important snapshot into the salience of security measures present in airports.

In this case study we focus on the positive and negative salience of security measures, as well as on the perceived (subjective) setbacks of security measures. First, let us look at the general salience of security measures (the analysis is based on passenger's indication of security measures as important during security procedures, Figure 3). Among the security procedures, six general salience clusters can be identified. First is the most salient security measures – led by metal detectors (over 54 %), followed by X-ray screening and CCTV. Second is medium salience of security personnel (over 41 %) and full body screening (i.e. the use of 3D body scanners). At low salience is hand search (almost 20%).

[9] *"Passengers who had experienced the scanners were often dissatisfied with the quality of service. They described scenes of confusion, undignified situations with security staff behaving in a bullish way, making an impression that passengers could not refuse to go through a scan, or even suspicious selection criteria applied by airport screeners"* (Beláková 2013b: 35).

[10] D4.4, Annex 7, Comparative report.

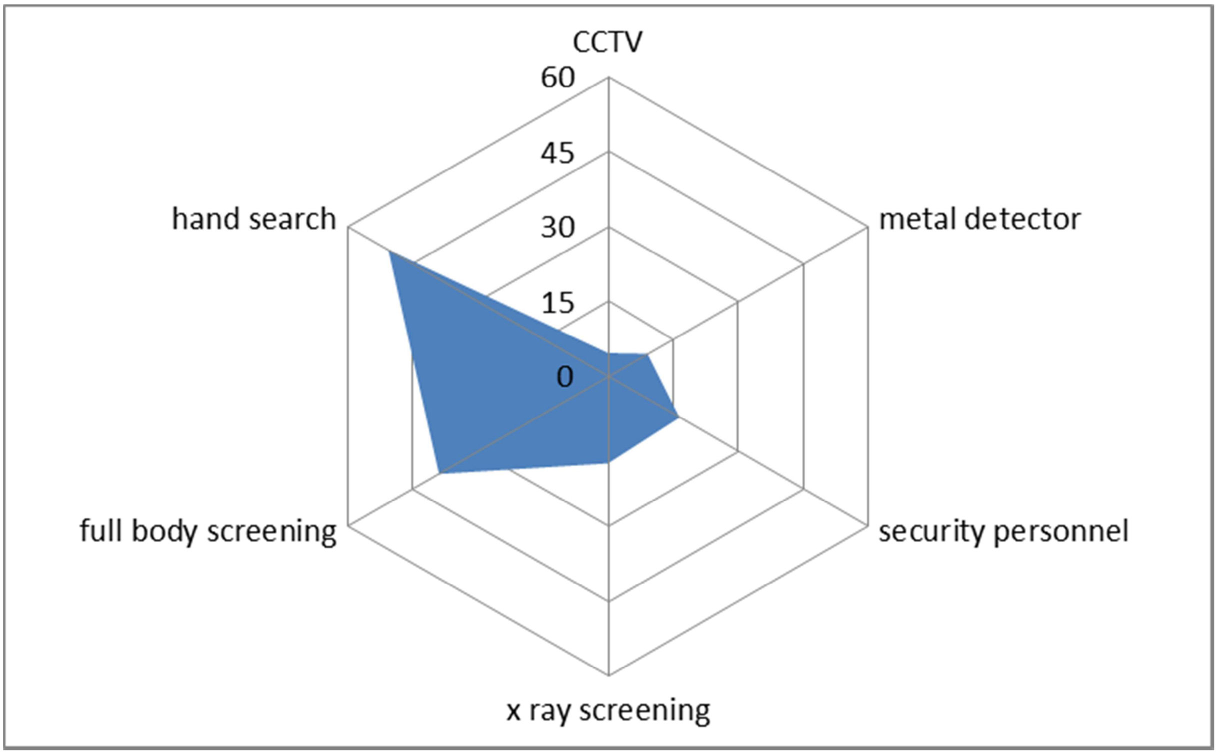
[11] Survey has been developed and put into practice by academics from the Facultys of Aeronautics, Anadolu University, Eskisehir, Turkey, and coordinated and performed by Dr. Nalan Ergun, Birsen Acikel and Dr. Ugur Turhan.



Note: N= 869
Source: Anadolu University

Figure 3: General salience of security procedures (in per cent)

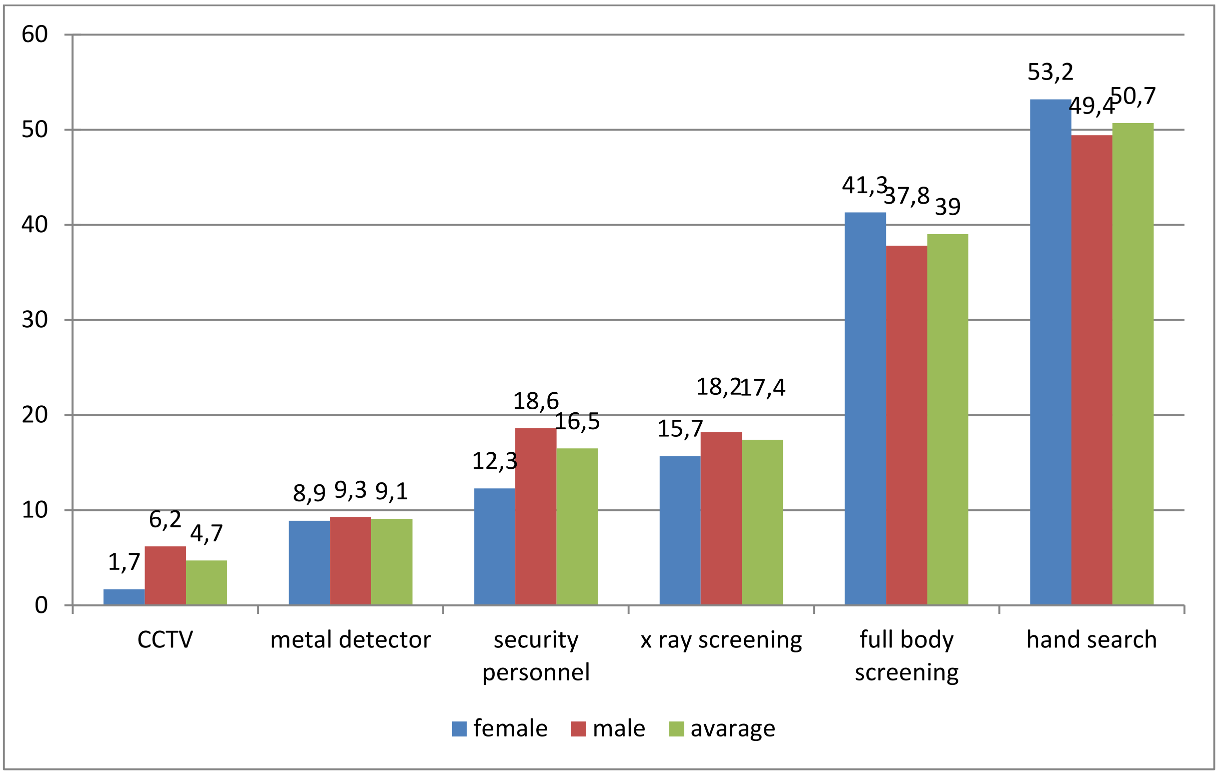
In the analysis of this question, we find significant differences based on socio-demographic variables such as age (passengers between 20 and 40 years of age view security measures as more salient), gender (male passengers tend to view security measures as more salient, as compared to their female counterparts), religion (Christian and Muslim passengers are on average more sensitive to security measures than passengers belonging to other religions or no religion) and education (the higher the education the higher the salience of security measures).



Note: N= 872
Source: Anadolu University

Figure 4: Negative salience of security measures (in per cent)

In terms of negative salience (based on passengers' subjective evaluation of security measures as disturbing), three clusters of negative salience can be identified – high negative salience of hand search (almost 51 %) followed by full body screening (39 %); medium negative salience of x-ray screening (more than 17 %) and security personnel (16,5 %); and low negative salience of metal detector (9 %) and CCTV (almost 5 %). Looking at the clusters of negative salience, it is clear that the degree of negative salience reflects the degree of perceived intrusion into the personal and even physical sphere of passengers – the most negative being hand search, which presumes physical contact between passenger and security personnel, followed by screening by machine (viewed as more impersonal, however there is a clear distinction between 3D body scanners and x-ray screening, as the former has more than double the negative salience of the latter), to a relative high acceptance (low negative salience) of non-contact security measures, such as CCTV and metal detectors.

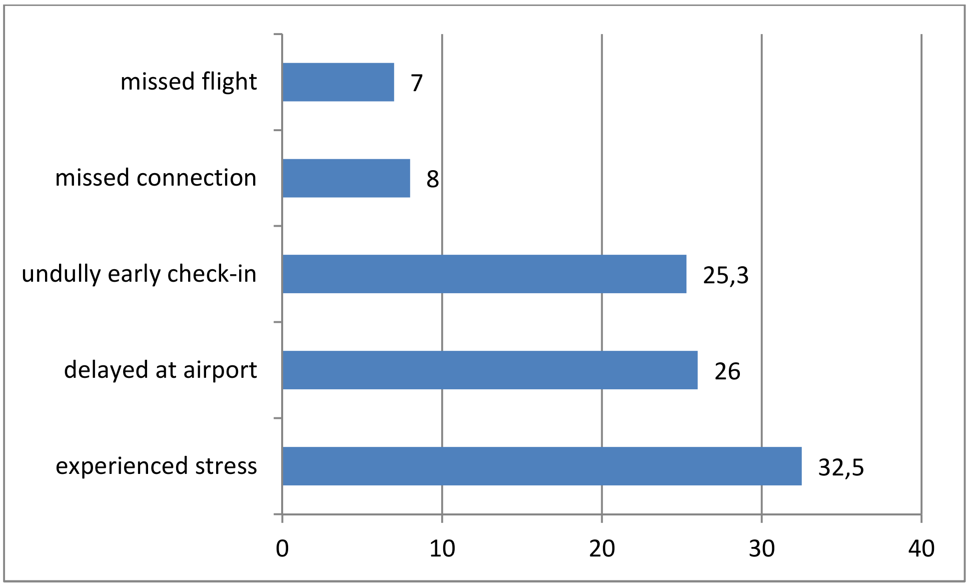


Note: N= 872
Source: Anadolu University

Figure 5: Gender differences in negative salience of security measures (in per cent)

In this respect negative salience is significantly influenced by cultural differences – different cultures have diverse conceptions of the private sphere and of the body (Moran et al 2007). In terms of socio-demographics, similar patterns can be found in the case of negative salience. As in general salience, we find significant differences based on socio-demographic variables, such as age (passengers between 20 and 40 years of age express stronger negative salience than their younger and older counterparts), gender (male passengers tend to view most security measures as more negatively salient, as compared to their female counterparts, with the exception of full body screening and hand search where female passengers show higher negative salience), religion (Christian and to lesser degree Muslim passengers express on average more negative salience than passengers belonging to other religion or no religion) and education (the higher the education the higher the negative salience of security measures expressed by passenger).

Figure 5 offers a more detailed look at the gender differentiation of negative salience of security measures – in the high negative salience pattern, women express stronger negative salience than man – both in regards to hand searches and to full body screening. On the contrary, male passengers express stronger negative salience in the medium and low negative salience patterns –in respect to x-ray screening, security personnel, metal detectors, and CCTV. These results hint at the need of airport authorities to consider passengers basic socio-demographic characteristics in order to successfully implement and perform security measures.



Note: N= 882
Source: Anadolu University

Figure 6: Negative effects of security measures (in per cent)

Figure 6 above, offers a more detailed insight into the negative salience of security measures. In general, 40% of passengers indicated having experienced negative effects from security measures – most passengers indicated experiencing stress (more than 32 %), delay at airports and unduly early check in (26% and more than 25%, respectively) and a small proportion of passengers missed their connection or flight (8% and 7%, respectively). The socio-demographics match those of the general and negative salience described above.

Model validation

At the airport models validation workshop held at Anadolu University in February 2014, this model (Table 2) was introduced to the participants who then were asked to assess it in general terms of usability, as well as the values of the individual categories given their experience and background. In total ten respondents provided detailed feedback, whose analysis can be summarised as follows.

Table 2: Model based on the effects of security measures in airport case study

Type of security measure		Cost		Profit		Effect on customer Acceptance/ Salience
Duration		short-term	long-term	short-term	long-term	n/a
Human resources	Hand search	High	medium	low	low	Negative (low salience)

	Security personnel	High	medium	low	low	neutral/rather positive (medium salience)
Technical resources	CCTV	High	low	medium	medium	positive (medium salience)
	Metal detector	High	low	medium	medium	positive (medium salience)
	X-ray	High	low	medium	medium	neutral/rather positive (medium salience)
	3D body scanner	Very high	low	medium	medium	negative (medium salience)

Source: IS AS CR

Note: Detailed explanation of the individual categories of the airport security acceptance model in Appendix I.

As seen in Table 3, differences can be observed between the assessment of the costs by the research team and by the respondents. The value medium assigned by the respondents to the short-term cost categories of hand search, security personnel, CCTV, and metal detectors can be explained by the fact that, compared to the general airport costs, the above mentioned categories do not represent great expenditures.

Table 3: Cost conceptual model and validation results

TYPE OF SECURITY MEASURE		COST (validation)	COST (model)	COST (validation)	COST (model)
DURATION		SHORT-TERM	SHORT-TERM	LONG-TERM	LONG-TERM
HUMAN RESOURCES	1. HAND SEARCH	medium	high	medium	Medium
	2. SECURITY PERSONNEL	medium	high	medium	Medium
TECHNICAL RESOURCES	3. CCTV	medium	high	low	Low
	4. METAL DETECTOR	medium	high	low	Low
	5. X-RAY	high	high	medium	Low
	6. 3D BODY SCANNER	high	high	medium	Low

Source: ISAS CR, data Seconomics validation workshop

As for the value "low," assigned to the long-term cost of X-rays and 3D body scanners, the difference is explained by similar justifications as above and by the fact that the technology's use has relatively low maintenance costs compared to other technologies employed by airports.

Table 4: Profit conceptual model and validation results

TYPE OF SECURITY MEASURE		PROFIT (validation)	PROFIT (model)	PROFIT (validation)	PROFIT (model)
DURATION		SHORT-TERM	SHORT-TERM	LONG-TERM	LONG-TERM
HUMAN RESOURCES	1. HAND SEARCH	low	low	low	Low
	2. SECURITY PERSONNEL	medium	low	medium	Low
TECHNICAL RESOURCES	3. CCTV cameras	low	medium	medium	Medium
	4. METAL DETECTOR	medium	medium	high	Medium
	5. X-RAY	medium	medium	high	Medium
	6. 3D BODY SCANNER	low	medium	medium	Medium

Source: ISAS CR, data Seconomics validation workshop

As in the comparison between the conceptual model and the validation of costs, the validation of profit shows variation between conceptual models and the perception of airport security experts. Above in Table 4, we see that the short-term profits of security personnel are perceived as medium by the experts, whilst being seen as low in the model. In turn, CCTV cameras' and 3D body scanners' short-term profits are viewed as low by the experts. In the long term the experts in the validation assigned high profits to metal detectors as well as X-rays, and medium profit to security personnel, CCTV and 3D body scanners.

Table 5: Comparing salience in the conceptual model, survey findings and validation

	salience	model validation
CCTV cameras	positive	Positive
metal detector	positive	Positive
security personnel	neutral	Neutral
X-ray screening	neutral	Positive
full body screening	negative	Negative
hand search	negative	Negative

Source: ISAS CR, data Anadolu airport Survey and Seconomics validation workshop

The last category compared is the salience of the individual security measures. This is the most important category in the Seconomics research on the perception and acceptance of airport security measures. In the validation, the feedback of airport security experts was very positive and the salience of security measures, which encompasses passengers' attitudes, was seen as both novel and beneficial in terms of the future planning of security cost allocation.

In Table 5, we clearly see that unlike in the categories of costs and profit, the salience conceptually modelled and measured in the Anadolu survey shows a high degree of similarity with the opinion of experts. The only exception being X-ray screening, whose salience is perceived as positive by the airport security experts in the validation but as neutral by the passengers in the Anadolu survey. Both our analysis and model validation categorise the metal detector and CCTV cameras as positive, security personnel as neutral and full body screening (3D body scanners) and hand search as negative.

4.2. Case study of salience of security measures: Critical infrastructure and Stuxnet

Unlike the two other security issues, Stuxnet is not a technology that directly affects the daily life of common people. The aim of Stuxnet is not to improve the security of individuals, as CCTV does by monitoring public spaces, or as 3D body scanners do by detecting weapons and preventing terrorist attacks. In fact, Stuxnet is a weapon itself. It was not developed to protect critical infrastructure, but, on contrary, to destroy it. Of the three security topics studied in our comparison, Stuxnet has the greatest impact on geopolitical stability and raises the biggest questions concerning international law and security. While changes at the macro level have large implications for the security and lives of individuals, its salience at the micro level seems to remain indirect and marginal today.

Cyber security is an important topic at the EU level, as it is more efficient in coordination and cooperation. Recently the EU has led a broad discussion of cyber-space protection, cyber security, and future developments in the field. It has also discussed possible regulations; whilst maintaining state sovereignty as a paramount. Our analysis provides some important insights into the current nature of cyber security media reporting and debate.

Unlike in the case of airport security and public transport security, there is no passenger or customer data available and applicable in the study of critical infrastructure security.[12] Therefore, we focus on the media salience of Stuxnet as a proxy to assess perceptions and attitudes about critical infrastructure and provide an in-depth comparative analysis of the issue across nine countries (for more information on the method, case, and media selection see D.4.4.).

The Stuxnet case is unique among our three topics in the media analysis due to its technical character. The debate was conducted almost entirely on the level of state

[12] Due to the virtual non-existence of primary data, our D4.2. analysis concentrated on a secondary analysis of survey data of attitudes towards risks related to nuclear energy, as well as attitudes towards cyber security. The data available about critical infrastructure is a very sensitive issue. For example, there have already been tensions within National Grid over the publishing of utility pipeline maps for safety purposes versus withholding them for security reasons.

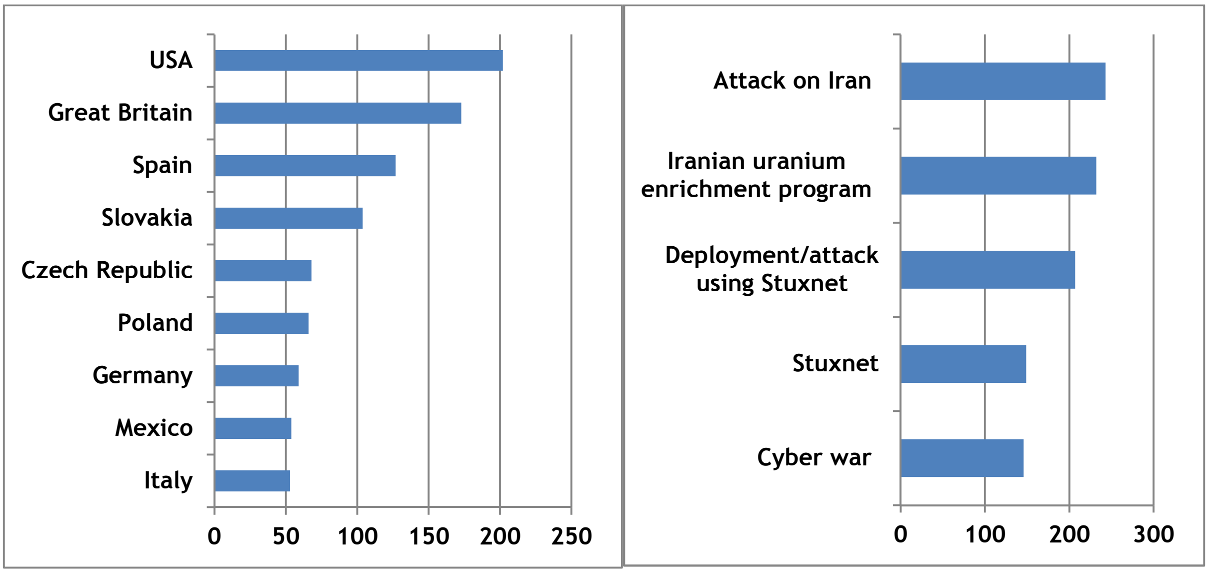
officials and experts, though journalists also provided some explanatory statements. Unlike in the other two topics (3D body scanners and CCTV cameras) the public and various civil society groups had only a marginal role in these media debates.

In terms of intensity as well as the nature of media reporting, the United States was indisputably the leading country and set the agenda for others. The reason for this is clear - Stuxnet, the computer virus used as a weapon to delay the Iranian uranium enrichment programme, was a domestic topic in the United States. Media in other selected countries followed the US debate, first by reporting on the character of the virus and explaining the situation, and second by evaluating and analyzing events that had occurred. The only country which provided an alternative perspective to that of the USA was Mexico, which feared it might be a future target of cyber-weapons. The remaining selected countries described events from the point of view of a detached observer.

The case of Stuxnet is relatively distant from individuals and thus does not attract strong media attention (except in the USA). In terms of risk perception, it is a direct threat to a state, rather than to an individual. Nevertheless the deployment of cyber-attacks in the future could have enormous consequences for the public and so it is desirable for people to be informed about these issues. In order to comprehend the complex nature of this issue, experts explanations and educational insights into complex matters of cyber security is desirable.

Three interconnected perspectives are typical to a certain extent in the media coverage of Stuxnet in counties under study (Figure 7).[13] The first and most prevalent perspective was the purely informative one. Here newspapers described Stuxnet and its functions and deployment and also wrote about the Iranian nuclear program. In general, the articles describing the virus were longer, more detailed, fact-filled, and contained the opinions of experts more often than the articles dealing with the functions of CCTV cameras and 3D body scanners.

[13] These levels of media perception of Stuxnet were described in the Italian report (de Gramatica 2013), but similar patterns also appeared in the majority of other countries.



Source: SECONOMICS ISASCR

Figure 7: Comparative assessment of salience by countries and main topics related to Stuxnet 2010-2013 (unit of analysis is number of articles)

The most salient topic in our comparative analysis was the “deployment - attack on Iran using Stuxnet” (in the figure above, on the right-hand graph this is the combination of the first and third category). This topic was relevant especially in the American, Slovakian, and Spanish press, which also paid a relatively large amount of attention to cyber-attacks in other states (Stuxnet also attacked critical infrastructure in Indonesia, India, Azerbaijan, and Pakistan). Remaining salient topics were rather general and descriptive – explaining the Iranian uranium enrichment program, Stuxnet, and cyber war.

Over time, the evolution of this perspective followed the international context of Stuxnet - the most attention paid to Stuxnet was from the first informative perspective in 2010 when newspapers wrote about virus itself, describing its functions and reported on the attack of the Iranian nuclear programme, and they also speculated about who developed this virus. In 2011 and 2012 newspapers focused on cyber-attacks in other countries and on the appearance of new viruses such as Flame, Stars, Duqu, and Red October, which were Stuxnet’s successors.

In the second perspective common in media coverage, Stuxnet was framed in the context of global cyber security, industrial espionage, and cyber war. The US played a leading role in writing about Stuxnet from this “macro” perspective, followed by Germany and Slovakia (Table 6). On this “macro” level – “in the grand scheme of things,” newspapers wrote about the wider consequences and negative effects of the Stuxnet attack on geopolitical stability, such as potential counterattacks, as well as the legitimacy of cyber-attacks in regards to international law.

Table 6: Categorization of topics according to salience 2010-2013

	Attack on Iran	Iranian uranium enrichment program	Deployment/attack using Stuxnet	Stuxnet	Cyber war
high salience	Spain	UK	USA	USA	Spain
	Great Britain	USA	Slovakia	UK	Czech Republic
		Slovakia	Spain	Germany	USA
		Spain			UK
medium salience	Slovakia	Poland	Italy	Czech Republic	Germany
	Germany	Czech Republic	Mexico	Italy	Poland
	USA			Mexico	Italy
					Mexico
low salience	Czech Republic	Germany	Germany	Spain	
	Italy	Italy	UK	Poland	
	Mexico	Mexico	Czech Republic		
	Poland				

Source: SECONOMICS ISASCR

Nevertheless, newspapers were entirely critical of Stuxnet and cyber-attacks in general. On contrary, the proponents of Stuxnet received quite lot of space, particularly in the US. In the US, Stuxnet proponents appreciated the complexity and efficiency of the virus and emphasized the security needs of their country. The Stuxnet attack was justified from global security perspectives with the motto, *“the best defence is good offence”* (Beláková 2013b). In other words, Stuxnet proponents considered the virus to be a quick and non-violent weapon, useful in pre-emptive strike which could prevent Iran from development of weapons of mass destruction. Moreover, cyber-attacks were for them less harmful and more cost-effective than armed conflicts.

The main concern regarding Stuxnet was the uncontrolled proliferation of and possible counterattacks in response to the virus, which entered the media debate in in 2011 and 2012. Critical voices warned against a worldwide proliferation of cyber weapons, which could represent dangers to critical infrastructure and to the industrial systems of many countries. The deployment of Stuxnet was, according to its American and Czech critics, similar to releasing a genie from a bottle or opening Pandora’s Box because in the future, Stuxnet could and would be modified and used for different targets world-wide. In this respect, Great Britain, the USA, Germany and Mexico felt endangered and vulnerable to possible attack.

Some critical viewpoints also appeared in media coverage of Stuxnet in Southern Europe (Italy, Spain) and in Mexico. Spanish newspapers considered Stuxnet to be a milestone in the process of cyber weapons development and noted that it marked a new kind of warfare, but also a new kind security threat. Although Mexican newspapers did not pay a lot of attention to Stuxnet, the perspective of the Mexican press is valuable for our comparison because it highlights questions about the legitimacy of cyber warfare and also viewed Stuxnet from the Iranian point of view. The Mexican perspective is exceptional because no other surveyed country gave so much space to the Iranian side of the conflict or considered Iran to be a 'victim of attack.' In fact, the general trend was to portray Iran as a 'callous culprit,' developing weapons of mass destruction under the guise of a peaceful nuclear programme. To a lesser degree, arguments concerning the legitimacy and legality of the Stuxnet attack were mentioned also in the Slovakian and American press, but the attention paid to these topics was not significant in the context of the whole debate.

Notwithstanding the critical voice of the Mexican media, Mexico, like most other countries, did often rely on the US for information, influencing the media portrayal of Stuxnet to a certain extent. The Mexican approach did not emphasise only one side of the conflict, did not marginalize the 'attacked,' and offered a broader array of arguments about the pros and cons of Stuxnet. It offered an important critical voice, standing against the majority, highlighting how easy it is for media in context of complex technical issues to rely on US reporting without asking critical questions.

The third "micro" level of reporting on Stuxnet was represented the least in countries from our comparison. Partly this approach was present in the United States, Italy, and Poland, but this perspective was only marginal there and certainly it did not dominate the security discourse in those countries. Nevertheless this perspective is important because it offers a new and more sophisticated viewpoint, not only of the issue of Stuxnet, but on cyber security at the micro level. This perspective contextualized Stuxnet in regards to the other methods of surveillance and personal data tracking. *"It dealt with the daily and often hidden reliance on services provided and supported by technology. Bank accounts, health information, internet communication, business, smart grids, and critical infrastructure services all depend to a great degree on an efficient and trustworthy technology system"* (de Gramatica 2013: 44). This third perspective shows us the reasons why Stuxnet is very relevant not only for information technology experts, security experts, and decision makers, but also and especially for the general population.

To summarize, in some countries, such as the United States, Germany, and to some extent also in Slovakia, all three perspectives or levels of media perception of Stuxnet were present. Generally speaking the debates in these countries were detailed and sophisticated. However, in most countries - especially the Czech Republic, Poland, UK,[14]

[14] Despite the relatively high media attention paid to Stuxnet in British media.

and Spain, media coverage of Stuxnet was reduced to one or two of the above described perspectives. Media in these countries provided mainly descriptive articles about Stuxnet while wider context and justifications of presented arguments were missing. In other words, newspapers answered the questions regarding actors, their country of origin, and topics, but failed to provide satisfactory justifications in respect to Stuxnet's legitimacy. Across all countries, any form of broader debate about the potential consequences and impacts of cyber-warfare were mostly missing.

4.3. Public transport and CCTV camera systems

The application of the model to public transport combines the SECONOMICS comparative media analysis data and passenger complaint data from an industry partner, TMB. In order to glean deeper insights from this cooperation special attention was paid to the particular context of Catalonia in the media analysis of the Spanish data. In fact, one national and one Catalan newspaper were selected to highlight regional differences.

4.3.1. Media Analysis and security measures

In an effort to address the tension between security and privacy within public transport, we studied the salience of the CCTV cameras issue in media. As the report D.4.4 showed, the attention paid to CCTV cameras in the public space differs. The US, Italy, Mexico, and, to some extent, Spain, are countries with low interest in the debate about CCTV cameras. We found great variation within the sampled countries, from high support and acceptance of CCTV cameras (in Poland, Slovakia, the Czech Republic, and Italy), to low attention paid to the issue, to rather negative attitudes towards the use of CCTV in public space (Germany and Great Britain).

We can also see dynamic developments in public opinion after dramatic events, as happened in the US after the attack on the Boston marathon in April 2013. According to our analysis, the perception of the CCTV cameras experiences a radical shift towards more acceptance every time some kind of terrorist attack occurs, but tolerance of the surveillance measures tends to vanish just as rapidly after the information about the attack leaves the media discourse (for more detail see Gawrecká et al. 2014). In the some countries, such as Spain and Italy, we didn´t see any broad discussion or controversy in the media.

In this topic, the Spanish media analysis national case study (Pereira-Puga, Hronešová 2013) will have an additional function. In the next stage the findings of the media analysis will be combined with the customer attitude survey of TMB in order to test the (possible) interaction between media saliency and customer attitudes towards security issues.

4.3.2. Case study of salience of security measures: Barcelona Metro

Spain has suffered severely from the financial crisis since its onset in 2008. The consequences of the world crisis have been more serious for southern Europe due to the structure of its economy, which is dependent on several commodities and services that were severely hit (for a detailed discussion see Taylor 2009). Spain's unemployment rose from 2,590,000 in 2008 to 5,769,000 in 2012, and then to over 6 million in 2013 (INE's Encuesta de Población Activa, EPA). Economic issues, and especially unemployment, thus outweigh security issues in the minds of most Spaniards[15] (see Pereira-Puga and Hronesova 2013).

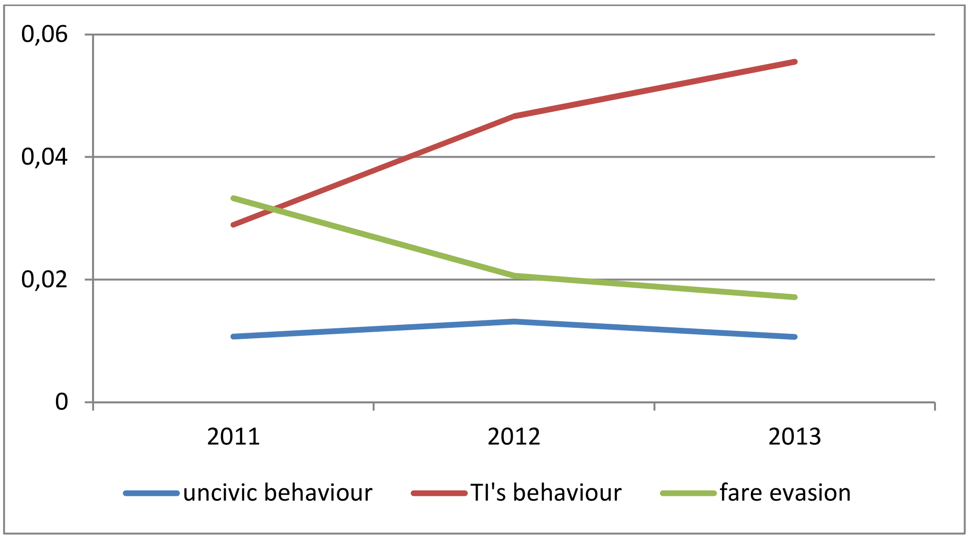
In our analysis of the salience of security measures on public transportation, we connect the media analysis results with the TMB data on reported security incidents and customer complaints and analyse them to provide insights into public acceptance of security measures.

Of the issues covered in our media analysis (see D.4.4.), CCTV camera systems were highly relevant to the TMB and was the most discussed issue in Spain. In fact it was even more frequently discussed in Catalonia, as demonstrated by the coverage of the issue in the Catalan daily newspaper, *La Vanguardia*. Unlike in the case of the body scanners, the debate on privacy vs. security was completely missing in media debates on the use of CCTV in Spain. The issue is uncontroversial, and CCTV cameras are quite well accepted by the majority of citizens, as long as data protection laws are not infringed. The main findings can be summarised as follows (for a more detailed analysis see Pereira-Puga and Hronesova 2013). First, state institutions, including the Catalan Data Protection Agency, the Madrid-based Commission of Surveillance, as well as city councils are quoted many times by journalists, providing information on the installation of new CCTV cameras in public places. Second, citizens support CCTV systems as a good measure to fight petty crimes. Nevertheless, it could be suspected that Spanish media try to muffle citizens' critiques of this technology. Third, the majority of actors quoted support the implementation of CCTV camera systems. And fourth, stakeholders consider video-surveillance to be a good defence strategy in the face of threats such as burglary or vandalism. However, they hardly mention terrorism as one of the potential risks.

The Critical Salience Index (Figure 8) is based on the annual data of the number of complaints combined with the annual data of the number of reported incidents per year and expresses the critical attitudes (i.e. negative salience) of passengers towards selected security issues. Overall, we identify very low negative salience for all three issues. However, one can identify variation among the individual issues over. The main findings can be summarized as follows: 1) over time the critical perception/rejection of

[15] This is an important change in Spain. Over a long history of violence and terrorism, Spanish governments have always placed security at the top of their political agendas. Indeed, even Spain's recent history includes plenty of acts of political violence. Nationalist groups such as the ETA in the Basque Country and the EPC in Catalonia, extreme left-leaning groups as the GRAPO, as well as extreme right-leaning bands as the GCR, have all mounted attacks in recent decades. Furthermore, Spain suffered the biggest jihadist attack in Europe in March 2004 when several bombs exploded on suburban trains in Madrid, causing almost 200 deaths (Sánchez-Cuenca 2007: 290).

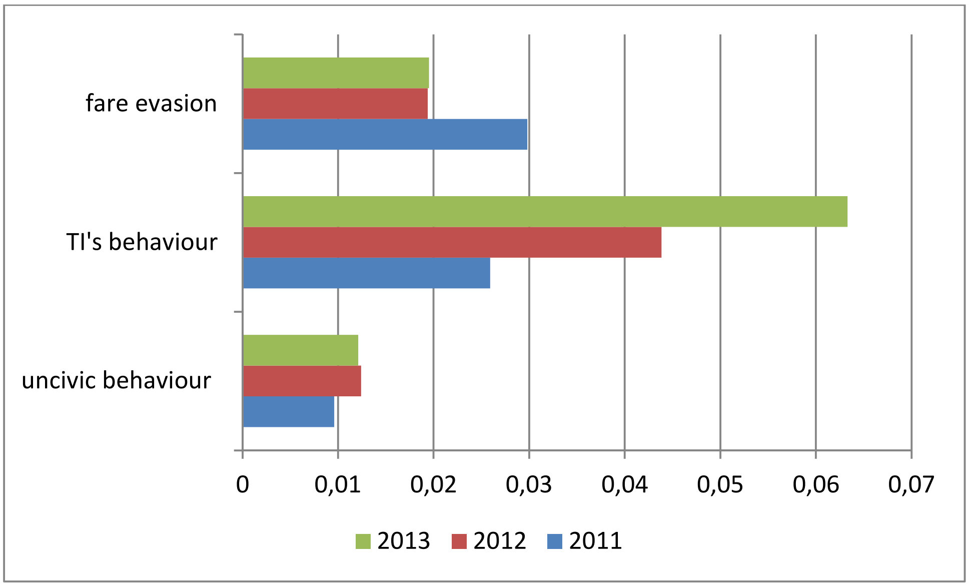
uncivic behaviour and especially of fare evasion decreases significantly; 2) critical perception of ticket inspector's behaviour grows over time.



Source: data TMB, analysis IS AS CR

Figure 8: Critical Salience of selected security issues over time (in degree of salience)

Further analysis will show the extent to which the critical salience is influenced by macro societal factors, such as the on-going crisis in Spain, or by specific factors, such as rising ticket prices on TMB. Furthermore, the critical salience index will be analysed along with customer satisfaction survey data from the TMB to provide further insight into the salience of security issues among TMB customers.



Source: data TMB, analysis IS AS CR

Figure 9: Comparing passenger complaints (negative salience) 2011-2013 (in degree of salience)

Figure 9 above provides more insights into the relevance of the selected issues among the overall complaints addressed to TMB by customers. Overall, the selected issues do not represent the main body of customers' concerns. Significant variation can be found among the three issues, with ticket inspectors' behaviour being perceived most critically by TMB customers and uncivic behaviour least critically. The number of complaints regarding fare evasion decreased significantly over time and hints at growing social tolerance of this form of behaviour. In the context of the on-going economic crisis in Spain, it can be hypothesized that fare evasion is more tolerated as the economic crisis affects customers. Along the same line of argument, in times of economic hardship customers become more aware of the costs of the ticket and their expectation of TI's behaviour rises, leading to more critical attitudes.

Based on the above mentioned results we could recommend together with WP3 a conceptual model, which in spite of the economic model (D5.2, version 1.0, p. 15-31) takes into account not only cost/investment and profit/efficiency, but also the effect on customer satisfaction and acceptance of security measures. The model is presented and described in D3.4.

5. Conclusion: New approaches to policy communication

The present study highlights the crucial role of media in providing information and (to a large degree) in shaping public opinion on security issues and measures (cf. Mazur 2006). All three case studies – airports, critical infrastructure, and public transport differ in their focus and target groups, but share an emphasis in existing and emerging threats, actual and perceived security, measures adopted to avoid these, and provision of good and reliable service. Simultaneously, all consider security costs and the sociological impacts of security measures and policy decisions, and take into account the public's reactions. In this respect all topics also relate to the media similarly. It acts as both a source of information and as an important means by which the public may from its general opinion, in both a positive and negative sense.

As for the application of the model to the airport case, the Anadolu Passenger Survey data analysis showed that both general salience and negative salience of security measures varies. Hand search and full body screening show the highest negative salience, whilst X-ray screening is significantly more accepted. It is therefore important for airport authorities to consider the salience of security measures, and in particular their negative salience, in their consideration of security technology (along with the cost and benefit analysis) and in the training of security personnel.

This is particularly true in respect to 3D body scanners, given the fact that its negative salience is double of that of X-ray screening, regardless of whether the benefits of this security measure outweigh its costs (both in terms of financial costs and passenger satisfaction). When considering body searches, which also have high negative salience, airport authorities must be sensitive to the diversity of passengers and their differing cultural perceptions of what is acceptable in searches, and then communicate that to security personnel during training. Increased sensitivity to passengers' diversity will increase the acceptance of security measures and improve overall satisfaction with airport security procedures.

The model validation showed that values in the categories of cost and profit can vary according to the context of the given airport. Important intervening factors are size, location, and the degree of modernisation at a given airport. The model validation shows that the salience of security measures is an important factor in considering their effect on the perception and satisfaction of passengers. The information on the salience of security measures, in particular negative salience, can be especially beneficial in training of security personnel, as strategies need to be developed to address passengers' concerns with security measures which are seen as intruding into their private sphere. The training of security personnel and effective communication with passengers could lead to the growth of positive responses from passengers.

To sum up, we have identified that in the field of airport security important factors that influence the salience of security measures are not only the nature of security measure itself, but also the explanation of the security measure to passengers by airport authorities, as well as the attention to and recognition of passengers' perspective and acceptance. In a time when airport travel is increasingly open to passengers of various ages, as well as social and cultural backgrounds, the challenge is for security authorities to recognize and address the diverse needs of these passengers and provide security whilst acknowledging and respecting the needs of passengers.

Concerning critical infrastructure, the media debate surrounding Stuxnet was very important[16] as it was the first transnational debate about cyber-attacks and cyber warfare. The media salience and resonance of Stuxnet also highlighted the degree to which cyber threats can affect everyday activities of citizens, such as online communication and sharing the information via social networks, internet banking, paying with credit cards, etc.

As for the application of the model to the public transport case, the main findings of the critical salience can be summarized as follows. First, CCTV cameras show high positive salience and are thus a readily accepted crime-prevention measure. Second, considering the most important categories of passengers' complaints, CCTV cameras are the best tool to address these problems. Third, overall we find low negative salience (complaints). Forth, there is a large degree of correlation between incidents and complains over time. This hints at the fact that an in-depth qualitative analysis of complaints could provide important insights into passenger's (security) concerns.

To conclude, this deliverable points to the distinction between actual and perceived security, as well as the difference between punitive and preventive security. Both have the potential to improve or weaken perceived security. It is therefore crucial, that transport operators take into consideration not only the possible effects of proposed measures on actual security, but also asses its acceptance and perception by passengers.

Beyond the scope of this report, but utilizing its findings is the WP5 and WP6 model validation. They use a combination of media and public opinion data in cooperation with UNITN (January – June 2014), which will be included in D4.5.

[16] Further details about Stuxnet can be found in D.4.4. and the SECONOMICS country reports.

6. Policy Recommendations

Our analysis demonstrates that effective communication of security risks and security measures is a critical task of contemporary governments and stakeholders. In this process media plays a crucial role in providing information, as well as being a platform for critical public debate of costs, benefits, and risks related to existing and emerging security threats and issues.

I. Today, security threats and security issues are no longer confined by the boundaries of nation states. On the contrary, they are both EU-wide and global. However, media reports on security issues remain largely written from a national perspective and shaped by domestic contexts. In this respect the EU can act as a bridge between the various domestic debates, bringing issues, such as emerging security threats like cyber security, to the European agenda.

II. In becoming a moderator of transnational security debates, EU institutions need to ensure the inclusive character of these debates, engaging policy makers, experts, as well as watchdog and civil society groups in order to facilitate their exchange of views on security issues.

III. There is an urgent need to increase the general understanding of emerging security issues. There is little awareness of what constitutes safe behaviour and an information campaign which would provide tailored information on various facets of online safety (i.e. for parents, for youth, for seniors, etc.) would be beneficial.

IV. Transport authorities need to consider the social acceptance of and attitudes towards security measures prior to their introduction as not doing this can raise new security threats (For example, in the public transport case study the introduction of sliding doors negatively affected social dynamics among passengers). Alternately, negative salience can contribute to the disruption of security procedures and outweighs the security benefits of new measures (as happened with 3D body scanners in the airport case study). Perceptions and attitudes of security measures ought to be considered when training security personnel.

V. Targeted communication must take into consideration the cultural and social diversity of the passengers (as demonstrated in the airport case survey) as well as acknowledge that the perception and experience of security can be affected by personal context (perception of security measures will change significantly between a single business traveller and family traveling with young children through an airport).

REFERENCES

Beck, U. 2002. “The Terrorist Threat. World Risk Society Revisited.” *Theory, Culture & Society* 19(4): 39–55.

Belakova, N. 2013a. “Surveillance Cameras Everywhere You Look? The portrayal of the Security vs. Privacy Dilemma in the Slovak Press, 2010 – 2013.” *Prague SECONOMICS Discussion Papers 2013/2*. [online]. Available from: http://www.seconomicsproject.eu/downloads.

Beláková, N. 2013b. “Drawing the line between security and privacy. An analysis of security discourses in the US press, 2010-2013.” *Prague SECONOMICS Discussion Papers 2013/7*. [online]. Available from: http://www.seconomicsproject.eu/downloads

Berry, D. 2013. *Ethics and Media Culture: Practices and Representations*. Burlington: Focal Press.

De Gramatica, M. 2013. “Better Naked than Dead. Communicating Security. Analysis of Italian Perception of Security Related Issues.” *Prague SECONOMICS Discussion Papers 2013/1*. [online]. Available from: http://www.seconomicsproject.eu/downloads.

Denton, R. E., & Woodward, G. C. (1990). *Political Communication in America*. New York: Praeger.

Edelman Trust Barometer 2013. *Annual Global Study. Executive Summary*. www.trust.edelman.com

Gawrecká, D., J. Hronešová, P. Vamberová, P. Guasti, Z. Mansfeldová. 2014. Comparative Analysis. Research report. Available from: http://www.soc.cas.cz/en/project/seconomics-socio-economics-meets-security.

Gawrecká, D. 2013. “Who Watches the Watchmen? Risk Perception and Security vs. the Privacy Dilemma in the Czech Press.” *Prague SECONOMICS Discussion Papers 2013/5*. [online]. Available from: http://www.seconomicsproject.eu/downloads.

Guasti, P., Mansfeldová, Z. 2013. “Perception of Terrorism and Security and the Role of Media”, paper presented at the The 7th ECPR General Conference, Section 55: Transnational Organised Crime in a Globalised World Governance, Organised Crime, Security, Terrorism, Panel 392: Transnational Organised Crime and Terrorism: Different Peas, Same Pod?, Bordeaux, 4 - 7 September 2013.

Habermas, J. 1996. *Between Facts and Norms*, Boston: MIT Press.

Hobbes, T. 1960. Leviathan: Or the matter, form and power of a commonwealth ecclesiastical and civil. Yale University Press.

Hronesova, J., Guasti, P. and Caulfield, T. J. 2013. “The Xanadu of surveillance: Report on security perceptions in the British online media.“ Contribution to the SECONOMICS project and Prague Graduate School in Comparative Qualitative Analysis 2013. Research report. Available from: http://www.soc.cas.cz/en/project/seconomics-socio-economics-meets-security http://www.edelman.com/insights/intellectual-property/trust-2013/

Inglehart, R. 1997. *Modernization and Postmodernization: Cultural, Economic and Political Change in 43 Societies*. Princeton: Princeton University Press.

Insights from the PRISE project on the public perception of new security technologies in Spain. Vienna, Institute for Public Policy CSIC.

Journalists and Social Media. Eurobarometer Qualitative Studies. Aggregate Report. January 2012. http://ec.europa.eu/public_opinion/archives/quali_en.htm, accessed 27.1.2014.

Kiousis, S. 2001. Public Trust or Mistrust? Perceptions of Media Credibility in the Information Age. *Mass Communication and Society* 4 (4): 381 – 403.

Lacina, T. 2014. "Report on Expert Blogs Analysis." Contribution to the SECONOMICS project and Prague Graduate School in Comparative Qualitative Analysis 2013. Research report. Available from: https://trinity.disi.unitn.it/bscw/bscw.cgi/424630, http://www.soc.cas.cz/en/project/seconomics-socio-economics-meets-security.

Lippmann, W. 1946. *Public Opinion*. Transaction Publishers.

Moran, R. T., Harris, P. R., & Moran, S. 2007. *Managing cultural differences*. London: Routledge.

McNair, B. 2011. *An Introduction to Political Communication*. Taylor & Francis Ltd - M.U.A.

Munné, R., R. Ortega, M. Pellot, P. Guasti, Z. Mansfeldová, J. Cano. 2014. D3.4 – Model Validation.

Nitzche, A. 2013. "Country report Germany." Contribution to the SECONOMICS project and Prague Graduate School in Comparative Qualitative Analysis 2013. Research report. Available from http://www.seconomicsproject.eu/downloads.

Pereira-Puga, Manuel and Jessie Hronešová. 2013. "Risks and Security in Spanish Newspapers: The Cases of 3D Body Scanners, CCTV and Stuxnet". *Prague SECONOMICS Discussion Papers 2013/6*. [online]. Available from: http://www.seconomicsproject.eu/downloads.

Pereira-Puga, M., Hronešová, J. 2013. "Risks and Security in Spanish Newspapers: The Cases of 3D Body Scanners, CCTV and Stuxnet." *Prague SECONOMICS Discussion Papers 2013/6*. [online]. Available from: http://www.seconomicsproject.eu/downloads.

Ríos, D., J. Cano, A. Tedeschi, A. Pollini, U. Turhan, M. Pellot, R. Ortega, R. Munné, 2014. D5.2 - Case Studies in Security Risk Analysis.

Sojka, A. 2013. "Poland – a Surveillance Eldorado? Security, Privacy, and New Technologies in Polish Leading Newspapers (2010-2013)." *Prague SECONOMICS Discussion Papers 2013/3*. [online]. Available from: http://www.seconomicsproject.eu/downloads.

Sanchez-Cuenca I. 2007. „The dynamics of nationalist terrorism: ETA and the IRA“ *Terrorism Polit. Violence* 19(3):289–306

Vamberová, P. 2013. “I’ll Be Watching You. Communitacing Security and Privacy Issues in the Mexican Press.” *Prague SECONOMICS Discussion Papers 2013/4.* [online]. Available from: http://www.seconomicsproject.eu/downloads

World Nuclear Association, 2012. http://www.world-nuclear.org, retrieved 2 November 2012.

Woohyun S., Massacci, F., De Gramatica, M. Allodi, L., Hung, V., Williams, J. Ruprai, R. 2014. Report on Experimental Analysis, SECONOMICS D6.3, version 9.0.

APPENDIX I: Explanation of the airport security acceptance model

1. Costs

1.1. Human Resources Costs

Values: high - medium

Important note: the categories are not mutually exclusive, but cumulative:
High: need in personnel recruitment, initial training personnel (taking into consideration personnel turnover), additional/specific training (e.g. in connection with new technologies). This has to be included in company's HR development plan, as well as in medium to long- term strategy (increase/decrease of personnel in connection with new technologies);
Medium: regular costs i.e. wages;

1.2. Technical Resources Costs

Values: high - low

High: purchase (one-time cost), installation of new equipment;
Low: regular maintenance, ad-hoc repairs;

2. Profit

Values: **Low - Medium - High**

This is a relative category, based on increase/decrease of ticket sale-related profit **due to effectiveness of the HR/technical measures;**

3. Effect on Customer Satisfaction

Values: low - high; Direction: negative - neutral

This category is related to the effect the measure will have on:
customer satisfaction,
level of acceptance (decrease in negative salience, decrease in passenger complaints);