SECONOMICS

D4.5 The Price of Security: A comparative analysis of public attitudes to security and acceptance of risk

Zdenka Mansfeldová, Petra Guasti, Daniela Gawrecká, Tomáš Lacina (IS AS CR), Martina de Gramatica, Woohyun Shim (UNITN) Alessandra Tedeschi, Alessandro Pollini (DBL), Julian Williams (UDUR), Ugur Turhan, Birsen Acikel (AU), Ricard Munné (ATOS), Michael Pellot (TMB), Raminder Ruprai (NGRID), Andreas Schmitz (ISST).

Pending of approval from the Research Executive Agency - EC

Document Number	D4.5
Document Title	The Price of Security: A comparative analysis of public attitudes to security and acceptance of risk
Version	1.0
Status	final
Work Package	WP 4
Deliverable Type	Report
Contractual Date of Delivery	31.01.2015
Actual Date of Delivery	27.01.2015
Responsible Unit	ISASCR
Contributors	AU, DBL, UNITN, TMB, ATOS, UDUR, NGRID,ISST
Keyword List	Security, privacy, media, salience, CCTV cameras, 3D body scanner, Stuxnet
Dissemination level	PU

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	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

	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	16/05/2014	Draft	P. Guasti, Z. Mansfeldova (ISASCR)	Draft
0.2	**10/10/2014**	Draft	P. Guasti, Z. Mansfeldova, D. Gawrecka, T. Lacina (ISASCR)	Draft
0.3	2/11/2014	Draft	P. Guasti, Z. Mansfeldova, D. Gawrecka, T. Lacina (ISASCR), M. de Gramatica (UNITN)	Draft
0.4	15/11/2014	Draft	P. Guasti, Z. Mansfeldova, D. Gawrecka, T. Lacina (ISASCR), M. de Gramatica (UNITN)	Draft
0.5	11.12.2014	Draft	P. Guasti, Z. Mansfeldova, D. Gawrecka, T. Lacina (ISASCR), M. de Gramatica, W. Shim (UNITN), A. Tedeschi, A. Pollini (DBL), J. Williams (UDUR), A. Schmitz (ISST)	Draft
0.6	15/12/2014	draft	M. Pellot (TMB), R. Munné (ATOS) and R.Ruprai (NGRID)	Input validation
0.7	16/12/2014	draft	P.Guasti, Z. Mansfeldova, P. Vamberova (ISASCR)	Draft revisions
0.8	22/12/2014	draft	E. Chiarani (UNITN)	Quality check completed. Minor changes requested.
0.9	19/01/2015	draft	W. Shim (UNITN)	Scientific review completed. Minor changes request.
0.10	26/01/2015	draft	F. Massacci (UNITN)	Final review. Some changes requested
1.0	27/01/2015	final	P.Guasti, Z. Mansfeldova (ISASCR)	Innorporated scientific review and PI's reccomendations, final revisions, Finalization

INDEX

Executive summary 6
1. Introduction 9
2. Theoretical and methodological framework 11
2.1 Tensions between security and freedom 11
2.2 Methodology and data 11
3. Empirical chapters 13
3.1 CCTV cameras – All of Big Brother's Eyes? 14
3.2 3D body scanners 18
3.3 Stuxnet in printed media and security expert blogs 23
4. Comparative chapters 28
4.1 Beliefs on quality and value of security measures in air transport 28
4.2 Acceptance of Security Measures in Urban Public Transport 30
4.3 Acceptance of security measures in Critical National Infrastructure (CNI) 31
4.3.1 Future and emerging threats: cyber-crime 32
4.3.2 Stuxnet – a milestone in cyber-security 33
4.3.3 Pan-European coordination 33
5. Conclusions. Future and emerging threats. 35
5.1. Security and the media 35
5.2. Salience of Security in SECONOMICS Case Studies 36
5.3. The price of security 37
REFERENCES 39

Executive summary

More and more globalization is leading to new security risks and threats. A compromise of freedom, privacy and security is not only becoming harder to reach, but also more important. Media contributes to public perception and opinion. Thus the main objectives of WP4 were to study citizen's reaction to risks and their acceptance of security measures in public opinions, attitudes and media.

This deliverable is a theory-driven interdisciplinary exploration of empirical findings to compare international media with survey data, existing secondary international data and SECONOMICS models and the validation of the SECONOMICS models. It is a result of cooperation among partners form WP1, 2, 3, 4, and 6.

We synthetize the findings of our media research in the empirical chapters. New insights into the comparative study of CCTV camera systems and 3D body scanners in printed media are presented. Further a comparison of reporting on cyber security in printed media and expert blogs is done in these chapters. In the comparative chapters we combine the media and other data and integrate the main findings of the validation process of SECONOMICS models. In conclusions, we address the issues of future and emerging threats as well as provide policy recommendations.

In the course of the project we have developed and applied instrument for qualitative comparative analysis of security issues in the media, in order to conduct in-depth qualitative and quantitative analysis of media coverage; created SECONOMICS media corpus (covering the issues and countries indicated above); constructed salience index and model of public acceptance of security measures and validated these with stakeholders and experts in aviation, urban public transport and critical national infrastructure domains.

By applying and advancing the methods of qualitative and quantitative research, we are able to fill the gap in the study of security and security risks by presenting a comparison of the unique data (media, survey, macro data) of transnational security issues in three areas of critical infrastructure (air transport, public transport and critical national infrastructures in form of energy provision networks).

Our case studies include cyber-terrorism as an example of risk and 3D scanners and CCTV cameras as an example of security measures, although, as mentioned above, some media outlets framed Stuxnet as a security measure. The main factors shaping how the media report on security threats and security measures are past experience with a particular security threat and the probability of the country being targeted in the future. These factors account for the main differences in the extent of coverage dedicated to the issue in the different domestic media.

The media debates in the studied countries each prioritized a specific aspect of national security – in reaction to the effect of both global events (i.e. terrorist attacks) and domestic developments (economic and political). Countries that are generally more active on the international scene and/or have had a previous experience with domestic and international terrorism are generally more exposed to (and hence concerned about) potential terrorist attacks. In these countries (the UK, the US, Spain, and Germany) security measures are high on the policy agenda, as demonstrated by the prioritization of body scanners in airport security and intensified CCTV camera use in counter-terrorism. In countries with no real danger of a terrorist attack by (international/national) extremist groups (Poland, the Czech Republic, Slovakia), there is a low policy interest in advanced and costly security devices, such as body scanners at airports and CCTV cameras, are seen positively as a crime prevention measure.

In the salience analysis of airport security, we find, that acceptance of security measure in airport context is connected with the perception of effectiveness of the given measure. Furthermore, the analysis shows that the perceived values of security procedures is enhanced by higher perception of quality, and affect the air-travel intention positively. Furthermore, we established indirect, but positive relationship between perceived equity, conceptualized broadly as different treatment due to passengers' nationality, and intention to travel.

The study of salience of security measures in urban public transport also yields highly innovative findings. Examination of critical salience index indicated very low negative salience of the three issues in question (fare evasion, uncivic behaviour – vandalism, and ticket inspectors' behaviour). The validation of the social model in urban public transport domain emphasized the need and importance of considering social factors in addressing security challenges both domestic and those of globalisation and growing diversity. Another aspect dominant during the validation activities was the need for comprehensive solutions to security issues.

Security coordination was an important point raised by stakeholders; within the various units of public transport provider, between different means of public transport (for example, effective implementation of security measure in metro can shift the security issue to public busses and vice versa), between public transport providers and security forces (Police), as well as pan European coordination of both public transport providers and of security forces (Police).

In regards to salience of Critical National Infrastructure security, SECONOMICS research highlights that both citizens and stakeholders largely underestimate the salience of security issues in the domain (D4.3, D4.4, D2.4). Furthermore, the validation in the CNI domain shown that salience and satisfaction of security issues have the potential to directly as well as indirectly influence costs of security.

Assurance and reliability of information for future and emerging CNI threats and appropriate dissemination of sensitive information are key challenges. The ways to mitigate some of the issues outlined above are ensuring that issues of citizens'

satisfaction are acknowledged and incorporated in allocation of resources, in training of security personnel, as well as substantially addressed in communication strategies of security stakeholders.

Events such as acts of terrorism (Boston marathon bombing 2013, terrorist attempt in Bonn 2013) can cause dramatic shift in salience of security measure – most interestingly shift from negative to positive salience (CCTV in both the US and Germany). However, as the initial shock subsides and the plurality of media debate returns to the initial level (after terrorist attack media are usually dominated by voices of actors favouring the monitoring of public spaces), the salience of the given security measure returns (almost) back to its initial standpoint. Hence while dramatic events such as acts of terrorism have the power to significantly influence public opinion, their impact is not as lasting as that of cultural attitudes and media landscape.

This deliverable highlights that the balance of security and freedom is the crucial task of contemporary governments, the role of critical media as a platform for public political discourse and as a guardian of freedoms is gaining considerable importance. Media play a critical role as an arena in which information is made available to the public, multiple claims and justifications are presented and discussed, and essentially opinions are formed.

1. Introduction

Globalisation and changes in society and the lifestyle of its members, including greater spatial mobility, have led to the emergence of new security risks and threats as well as significant changes in the general perception and acceptance of risk. Advanced modern societies and their members, while enjoying an unprecedented degree of existential security, are perhaps paradoxically concerned about security and safety (cf. Beck 1992, 2002; Giddens 1999; Inglehart 1997). Compared to the past, the new threats are mainly a product of human activity (Beck 1992; Giddens 1999); their repercussions are potentially much more severe, as they are not temporally, spatially or socially circumscribed in that they do not respect the boundaries of nation-states (Beck 2002).

The new risks have become one of the central dynamics of contemporary societies and are reshaping the current social order (Beck 1992). In response to the new kinds of security threats faced by postmodern societies, new methods of surveillance have been created. Despite their usefulness for strengthening security, these new methods of surveillance can pose a threat to people's privacy, dignity and health (Davis and Silver 2004). This represents a significant challenge to policy-makers in advanced democratic societies who are faced with demands for more security as well as opposition to the possible limitation of civil rights and democratic freedoms.

The interaction between security technology and public attitudes in part determines the effectiveness of different policy approaches and regimes. Risk-based models offer a means of adapting to new threats, but determining the correct auditing mechanism that sufficiently reassures stakeholders is a considerable challenge. In this case, the economic and public policy environments play an important role in determining the optimal regulatory structures.

The conflict between degrees of freedom and security is an increasingly important issue in the contemporary media. The media may to some extent influence how citizens perceive risks (Sjöberg and Vahlberg 2000) and aid in the acceptance or rejection of security measures. Media contribute to the public perception of security threats because they frame the communication surrounding security problems by focusing on 'what will be discussed, how it will be discussed, and above all, how it will not be discussed' (Altheide 1997, 650).

The deliverable is a theory-driven interdisciplinary exploration of empirical findings from diverse fields, whose aim is to compare media with survey data, models provided by the SECONOMICS partners, and validation of SECONOMICS models.

The main objectives of WP4 Security and Society are to (1) study citizen's reactions to risks and their acceptance of security measures, (2) the interplay between security and risk in public opinion and attitudes, and (3) media framing of security and security technologies. This involves (1) examination of the salience and acceptance of security measures, of the tension between security and privacy, (2) mutual trade-offs of risks

and security for citizens, as well as (3) the identification of effective channels and patterns of communication on security and risk.

Over the course of the SECONOMICS project, we have collected and analysed secondary quantitative data on risk perception and security (D4.2). We have also collected and analysed media debates on three security issues (3D body scanners, Stuxnet and CCTV) in 20 major dailies of 10 countries over a period of 40 months (from January 2010 to April 2013) (D4.4). We then synthesised media analysis results with customer surveys data (from airports and public transport), customer complaints data (from public transport), and expert interviews and ethnographic observation (from airports) (D4.3). Finally, we developed conceptual models combining cost, profit and effects of individual security measures on customer acceptance/salience (D4.3, D3.4, D2.4).

Over the course of the project, we have developed and applied an instrument for qualitative comparative analysis of security issues in the media in order to conduct in-depth qualitative and quantitative analysis of media coverage. We created the SECONOMICS media corpus (covering the issues and countries indicated above) and constructed a salience index and a model of public acceptance of security measures, which was validated with stakeholders and experts in aviation, urban public transport and critical national infrastructure domains.

By applying and advancing these methods of qualitative and quantitative research, we are able to fill the gap in the study of security and security risks by presenting a comparison of the unique data (media, survey, macro data) of transnational security issues in three areas of critical infrastructure - air transport, public transport and critical national infrastructures in form of energy provision networks. In the empirical chapters of this deliverable, we synthesise the findings of our media research, presenting new insights into the comparative study of CCTV camera systems and 3D body scanners in printed media as well as a comparison of reporting on cyber security in printed media and expert blogs. In the comparative chapters, we combine the media and other data and integrate the main findings of the validation process for SECONOMICS models. In our conclusion, we address the issues of future and emerging threats and provide policy recommendations and specifically identify issues for pan-European coordination.

2. Theoretical and methodological framework

In order to capture the dynamic character of contemporary security, we must first introduce the theoretical concepts and methodologies included in this deliverable. Here the main focus will be to show how various approaches (sociological, media research, etc.) contribute to a deeper understanding of the challenges facing contemporary societies (and policy makers) in their efforts to balance security, its financial costs, privacy and freedom.

2.1 Tensions between security and freedom

Decision makers in democratic societies are increasingly facing tensions between ensuring security and the trust and satisfaction of their citizens. The main reason is that satisfaction is not only connected to the absence of fear and feeling of safety, but also to absence of (perceived or real) far reaching security measures infringing upon privacy and (the feeling of) freedom.

The dilemma of our times, for governments, the media and individual citizens, is thus the question of how much safety and security we desire and at what price. In this dilemma, the media plays a critical role as an arena in which information is made available to the public, multiple claims and justifications are presented and discussed, and essentially opinions are formed.

With the growing internationalisation and transnationalisation of media, political arenas are transcending boundaries of nation-states and political communication is undergoing profound changes. Comparative research can thus provide crucial insights into similarities and differences in communication patterns during times of profound change in reporting and communication of safety and security issues.

2.2 Methodology and data

For the purpose of this study, salience is defined as the public perception and reception of security issues and specifically for security measures. For this purpose, salience signifies the degree of acceptance (positive salience) and the degree of rejection (negative salience).

We distinguish 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 a comparative media analysis and supplemented by data from customer surveys (from airports and public transport) and customer complaints (from public transport). Our extensive research confirms that in order to successfully communicate high acceptance and low to medium salience, or high salience (but predominantly positive) is needed for the security measure to be accepted by the public/customers/passengers.

Media sample

The articles analysed in the study were all drawn from the period between January 2010 and April 2013. Each article was sourced from the two most circulated, quality dailies (i.e. mainstream newspapers) in the following old and new EU member states: The Czech Republic, Germany, Italy, Poland, Slovakia, Spain and the United Kingdom (UK). Articles were also sourced from non-EU member states important in either shaping the global discussions of the selected issues (the United States (US)) or key in providing relevant cultural diversity (Turkey and Mexico). Four expert security blogs were also selected to provide insights into the opinions of the security expert community, in addition to the opinions of the general population provided by the articles. The twenty national newspapers selected provided over 2800 articles during the given period. The expert blogs contributed approximately 400 articles.

Case studies[1]

Three issues were identified as transnationally salient in the current media and relevant for comparative analysis: 3D body scanners, CCTV cameras and Stuxnet. 3D body scanners and CCTV cameras are highly relevant to the dilemma of security versus privacy. The debate over 3D body scanners at airports has highlighted the issues of the costs of security[2] and the potential health risks of security measures as factors that influence the perception and acceptance of a particular security measure. CCTV cameras are an example of a technology whose salience and social acceptance varies across different countries[3] (Lyon 2002). Stuxnet was selected as an issue because it introduced cyber-terrorism and certain vulnerabilities in critical infrastructure to public debate (Collins and McCombie 2012). From late 2010 up to the present, this topic has demonstrated its ability to be of significance for both policy makers and the public, generating debate in both general and special-interest media, namely expert blogs.

CCTV cameras and 3D Body scanners are technologies used to prevent traditional crime and modern terrorism as well as to detect perpetrators. However, another area in the field of security studies, criminology, and counter-terrorism has become salient in the discourse on modern security risks: cyber-crime. Cyber-crime uses information systems and technology to commit extortion, identity theft, espionage, or even to paralyse or destroy critical infrastructure (Collins and McCombie 2012). Though there have been many examples of these viruses in recent years, Stuxnet is not a technology that directly affects the daily life of ordinary people. Rather, 'Stuxnet, the computer worm which disrupted Iranian nuclear enrichment in 2010, is the first instance of a computer

[1] For more detailed information please see D4.3. and D4.4.

[2] Costs of security are here used in more general terms encompassing various types of costs (1) financial – implementation costs of new technologies, and (2) non-financial costs – security as a burden to public affecting acceptance of security measures.

[3] According to David Lyon (2002), surveillance, as one method of ensuring security, can be placed on a spectrum that ranges between 'care' and 'control'. At one end 'care' stands for watching over society for the purpose of its protection. 'Control', on the other hand, is about scrutinising people's behaviour to enforce discipline and order.

network attack known to cause physical damage across international boundaries' (Lindsay 2013, 365).

In response to media reports of the cyber-attack, many governments called for international coordination on cyber-security strategies while also trying to secure an advantage in cyberspace (Farwell and Rohozinski 2011, 31). The reason why Stuxnet has shaken public views of cyber-security is that it was unprecedented in its scope and effectiveness. The media labelled Stuxnet as 'the cyber equivalent of the dropping of the atom bomb' and claimed that it heralded 'a new era of warfare' (Lindsay 2013, 365) and a 'revolution in cyber-attacks' (Collins and McCombie 2012, 80). Stuxnet has also shown that using cyberspace against enemies involves lower costs and risks than traditional military means. In response to these developments, the British Government responded with the release of the National Security Strategy (NSS) and the Strategic Defence and Security Review (SDSR) in October 2010 and devoted over £650 million to bolster cyber-security (Cornish et al. 2011). However, a clear roadmap that would structure the best practice and assure transparency in cyber-protection is still under development.

3. Empirical chapters

In this part of the deliverable, dedicated to media analysis, we focus on the presentation of discourses and justifications of the media in transmitting information and shaping attitudes towards security issues and security measures. This section focuses on a comparative analysis of the discourses and the justifications of security and risk in domestic and international media in connection with three cases of critical infrastructure. The identification of effective channels and patterns of communication and risk prevention for specific target groups is a fundamental topic that needs to be explored. This section is based on the results of individual country reports and a comparative analysis of domestic and international media in 10 countries and in expert blogs (Belakova 2013a,b; De Gramatica 2013; Gawrecká 2013; Gawrecká et al. 2014; Hronešová, Guasti, Caulfield 2014; Nitzche 2013; Pereira-Puga 2013; Sojka 2013; Vamberová 2013).

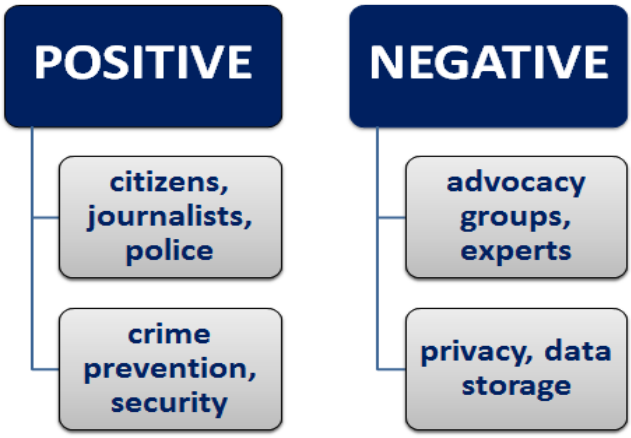
In this section, we fill a gap in the study of security and security risks by presenting a comparison of the coverage of transnational security issues in the media outlets of ten countries. We find that the media landscape, although fragmented and largely confined to the boundaries of nation-states, is undergoing a transformation as the importance of international context grows. At the same time, the media is shifting from a focus on security threats to an awareness of the possible trade-offs of security measures in terms of health, privacy, freedom, and civil liberties. Security related-issues, such as surveillance, the right to privacy, and the protection of that right are not clearly defined in static terms. Rather, their perception is influenced by the security context, mass media, cultural variables, laws, and particular context of each specific state. Simultaneously, the public is becoming more sensitive not only to threats but also to the costs of security.

3.1 CCTV cameras – All of Big Brother's Eyes?

This chapter analyses media coverage and perception of closed-circuit television (CCTV) cameras. The aim is to compare and describe main tendencies and specific factors in the debate on surveillance cameras, the arguments of the most salient actors, and also to contextualise the topics and justifications that appeared in the newspapers of ten countries.

We found that CCTV cameras received more attention than the cases of 3D body scanners and the computer virus Stuxnet. Among the countries under study, there was no dominant country which shaped the debate in the European and worldwide context or framed the discourse for others. Unlike Stuxnet and 3D body scanners, CCTV cameras were not particularly salient issues in the US media. On the contrary, Polish, Slovakian and German debate was rich, vivid and heterogeneous. In Poland and Germany, CCTV cameras were the centre of much media controversy. Poland belonged to the strongest proponents of CCTV cameras while German articles revealed a mainly negative attitude towards these devices. In Italy, Spain and Mexico, the debate was poorest and the most shallow of the ten countries under study with no broader discussion or controversies in the media.

CCTV cameras were considered a domestic issue whose influences and effects existed within the confines of each country. Newspapers rarely quoted information from foreign media or press agencies and relied on their own sources. Articles on cameras were predominantly informative and mostly shorter than in the cases of 3D body scanners and Stuxnet. The media mainly focused on specific crimes that were captured by CCTV cameras, with no broader reflection of the cameras' advantages and disadvantages. Figure 1 summarises opinions of the most important actors (both proponents and opponents) of CCTV cameras. In the second box in each column, the most salient actors in the debate are mentioned. The third box presents their arguments and concerns.



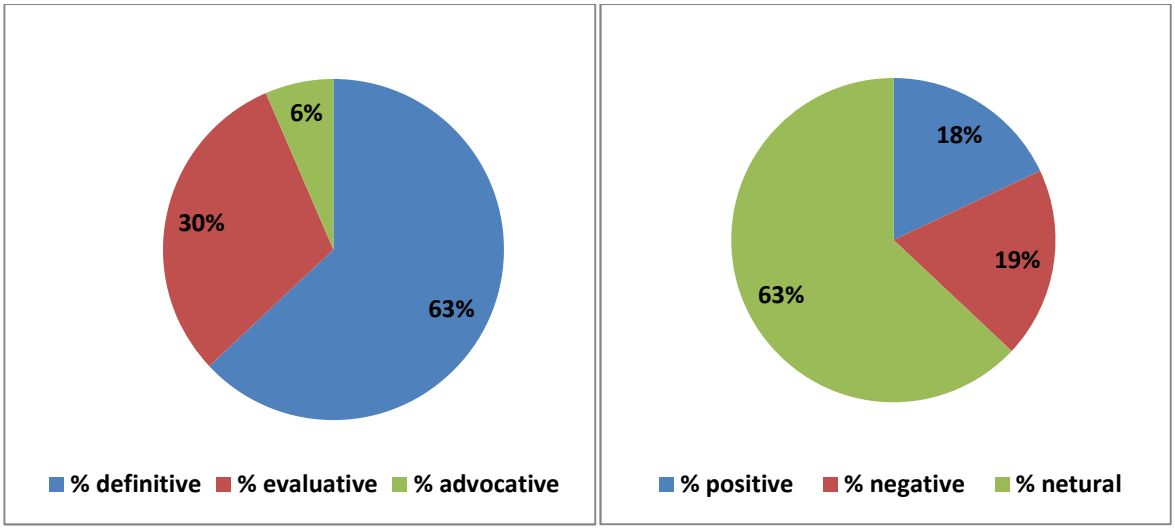
Source: SECONOMICS ISASCR

Figure 1 – General tendencies: Evaluation of CCTV cameras by the most important actors

In Figure 1 we can see that the coverage of CCTV cameras was framed mainly by the opinions of 'journalists' who dominated the debate in seven countries. They did not inform the public in a neutral tone and directly influenced the debate by offering their mostly positive opinions and commentaries on CCTV cameras. Other salient actors who made statements in articles about CCTV cameras were various 'state institutions', 'police' 'passengers' and 'citizens' who mostly supported the installation of these devices by pointing toward increases in security.

Civil society and advocacy groups were not presented among the top actors in the articles about CCTV cameras. Despite this, they played a salient role in the debate because of their critical view on cameras. Psychologists, university professors and other experts posed similar opinions against monitoring in the debate as advocacy groups.

The dominant narrative strategy used in the articles was definitive and the prevailing tone of evaluation was neutral. Nevertheless, discussion surrounding CCTV cameras contained a relatively high number of evaluations[4] in comparison to Stuxnet and 3D body scanners. Negative evaluation of CCTV cameras prevailed slightly over positive evaluations. Nonetheless, this difference was not significant and the number of arguments between opponents and supporters was more or less balanced (see Figure 2).



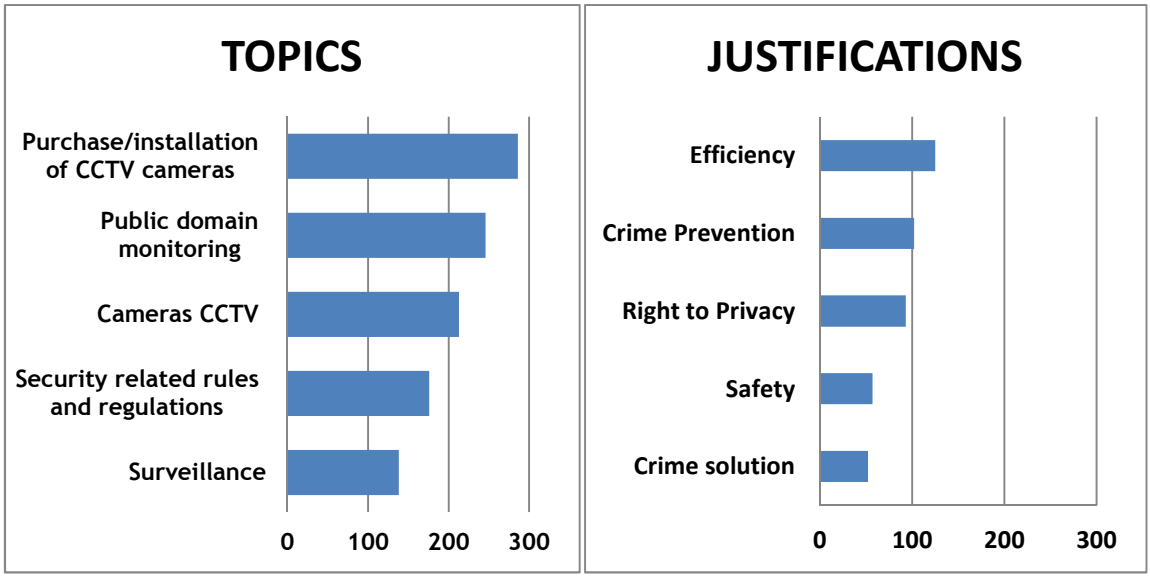
Source: SECONOMICS ISASCR

Figure 2 - Argumentative strategies of and evaluations of CCTV cameras

[4] One third of the coded statements were evaluative.

The prevailing topics discussed in the analysed articles were the 'purchase and installation of cameras' and 'public domain monitoring', which appeared mainly in short and non-analytical articles and were often connected with the justifications of 'efficiency', 'crime prevention' and 'privacy'. Other salient topics were 'surveillance' and 'security related rules and regulations', which were often mentioned together. Newspapers also paid attention to 'security rules and regulations' connected with negative aspects of surveillance technologies, for example the endangerment of privacy. The media in this regard called for better legal regulations of CCTV cameras.

The dominant justifications used by proponents of CCTV cameras were the 'efficiency' of camera systems in the fight against crime and their ability to strengthen security (see Figure 3). The security aspect of CCTV cameras was salient for more than half of the countries in our comparison (Germany, the USA, Spain, Poland, Slovakia, and the Czech Republic). Nevertheless, the efficiency of cameras was often questioned. In Italy, newspapers pointed to the fact that the camera's costs were often subsidized and that is why camera systems were sometimes installed regardless of their efficiency. Opponents of CCTV cameras often pointed to the fact that camera systems endangered rights to 'privacy' and personal freedom. Similar to 3D body scanners, issues of data storage and their potential misuse were mentioned.



Source: SECONOMICS ISASCR

Figure 3 - Comparative assessment of salience by main topics and justifications related to CCTV cameras

Analysis of topics and justifications revealed that the media were aware of the trade-offs between security and privacy in regard to CCTV cameras. Nevertheless, opinions on the surveillance of actors differed on a security-privacy axis from country to country as well as the price of security that they were willing to pay. This price depended on

following five dominant factors which framed the debate and (de)legitimised the extensive use of cameras in public eye:

(1) **CAMERAS AS A TOOL OF PROGRESS, MODERNISATION AND SECURITY**. In this aspect, a division was visible between old and new EU member states. New member states of the EU, especially Poland (which represented a rather uncritical view on security technologies in the debate), Slovakia and partly also the Czech Republic focused heavily on the CCTV cameras issue. They exhibited an especially high level of interest in the cameras' purchase and installation. Particularly in Poland, cameras became a symbol of social status and modernisation. Citizens were almost proud of being monitored because they considered it to be modern. In other words, CCTV cameras were a part of the discourse of 'catching up with the West'. However, since 2012 (see Figure 4) the debate has become deeper and more sophisticated. Newspapers have questioned the efficiency of cameras, pointed to the lack of privacy, and emphasised the need for clear legislative regulation.

(2) The opposite trend of **SECURITY TECHNOLOGIES AS A POTENTIAL THREAT** was typical for the old EU member states and was clearly visible in Germany and the UK. These countries, which have long-term experience with CCTV cameras, were aware of their advantages and disadvantages and reflected more on the issue of balance between security and personal freedom and on the negative aspects of camera use. This cautious attitude toward surveillance technologies and methods is a typical feature of the German security debate and is sometimes called 'Deutsche Angst' (German hesitancy).

(3) **PREVIOUS EXPERIENCE WITH TERRORISM** was another aspect influencing the acceptance of CCTV cameras. It was visible in the United States and Germany, where public opinions on cameras have undergone a dynamic development due to terrorist attacks or their attempts. At the beginning of the studied period, CCTV cameras were perceived rather negatively in the United States and citizens did not pay much attention to the issue. After the attack at the Boston Marathon in April 2013, where CCTV cameras played an important role in the identification of the culprits, the general public started to be more tolerant towards CCTV cameras. Similarly, public acceptance of CCTV cameras increased slightly in Germany after an attempted attack at the main train station in Bonn in December 2012 (see Figure 4).

Source: SECONOMICS ISASCR

Figure 4 - Timeline of development of topics and justifications

(4) **LOCATION OF MONITORING** played an important role in media acceptance of CCTV cameras. The attitude of the press towards 'private domain monitoring' in schools, hospitals, work places, housing estates, and prisons was much more critical than towards the monitoring of public spaces such as streets, traffic infrastructure or public transport. This difference between public acceptance and refusal of private monitoring was particularly salient in Slovakia, Poland and Spain.

(5) The last aspect influencing media perception of CCTV cameras was a **BAD INNER-SECURITY SITUATION**, either real (as in the case of Mexico which has faced long-term problems with high crime rates and a war between drug cartels and the police) or perceived (less serious crimes such as acts of vandalism, pickpocketing, or violence in football stadiums which were particularly reflected in media debates in Poland, the Czech Republic and Slovakia).

3.2 3D body scanners

In the domain of civil aviation, security-related issues are extensively debated and broadly addressed. While security measures have been mostly provided in the form of technological devices (X-ray machines, metal detectors, CCTV cameras, security wands), lesser efforts have been made to investigate the problem from the public opinion's point of view. Many studies (for example, Mackey 2007; Mackey, Smith 2012; Rajaonah et al. 2014; Tirosh, Birnhack 2013; Holguìn-Veras et al., 2012) indeed demonstrate that passengers' and citizens' perceptions and attitudes toward security measures strongly affect their behaviour and their choices with regard to the travel intention. Public opinion toward security and risk should therefore be regarded as a relevant aspect that is able to influence different security policy approaches and decisions.

The aim of this subsection is to analyse media coverage and the public opinion's perception of 3D body scanners, a highly debated aviation security measure under continuous revision. The purpose of the following research is to compare and describe the main tendencies and the specific factors identified in the media's recent public

discussion on this device as they appeared in newspapers from ten EU and non-EU countries from 2010 to 2013. Moreover, this study allows us to better understand how this specific debate is framed in the different countries considered, how the security issues are conceptualised and how the trade-offs generated by the increasing security procedures are perceived and shaped by the public opinion.

The analysis focused on the most frequent actors conducting the debate on the 3D body scanners, identifying the supporters and the opponents to the scanners' implementation, the most salient topics and justifications they used and the direction of the argumentations they claimed. The results of our analysis show that a crucial task is balancing all the trade-offs emerging between individual freedom and the security itself.

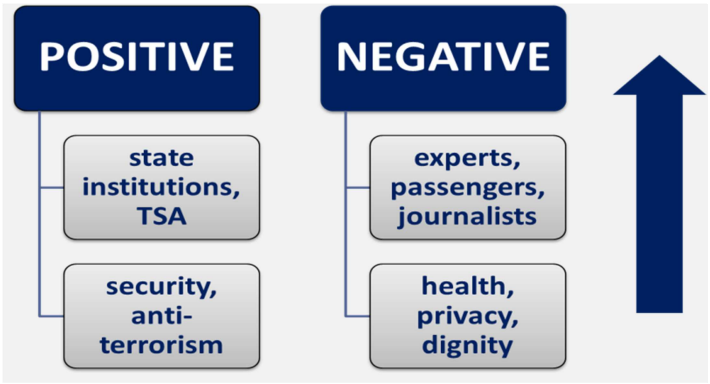
According to this research, the debate surrounding the 3D body scanners was more sophisticated and multifaceted than the debate on the CCTV cameras (3.1.) because it contained more analytical articles dealing with the broader international context of the aviation domain in a more sophisticated manner and was not limited to shorter informative articles (as in many cases of the articles on CCTV cameras).

Looking at the comparative data, the US was indisputably the leading country in the debate surrounding 3D body scanners, where the topic was lively and strong, followed by the UK, Germany and partly Italy, all countries where the device has already been installed. The predominance of the US in the debate is easily motivated when the approach of the American government over the last decade in regard to security issues is examined. Moreover, the US shaped and significantly influenced the reaction of the other countries included in our comparison at a global level on the 3D body scanner topic. The American debate indeed spilled over to many states. This trend was particularly visible in countries where the level of discussion was particularly low such as Mexico, Poland, and the Czech Republic.[5]

Despite differences among the countries under study, it has been possible to identify a common tendency in the classification of the actors (see Figure 5). Figure 5 presents two opposite factions in relation to actors, argumentative strategies, argumentative directions and justifications expressed by the national media analysed. The most salient actors in the debate on 3D body scanners are presented in the second box in each column and the third box contains their opinions and argument. Figure 5 show us that proponents of the scanners considered the machine as a necessary and effective tool for strengthening airport security in response to the increasing global terrorist threat, while opponents of the device mentioned three important arguments against scanners' usage,

[5] Media in these countries very often reflected the situation in the US and relied particularly on US media outlets such as The New York Times, CNN, and press agencies like the AP and DPA.

namely 'privacy,' ;'health[6],' and 'quality of service'. Arrow in the figure means that opinion of scanners 'opponents prevailed in the debate.



Source: SECONOMICS ISASCR

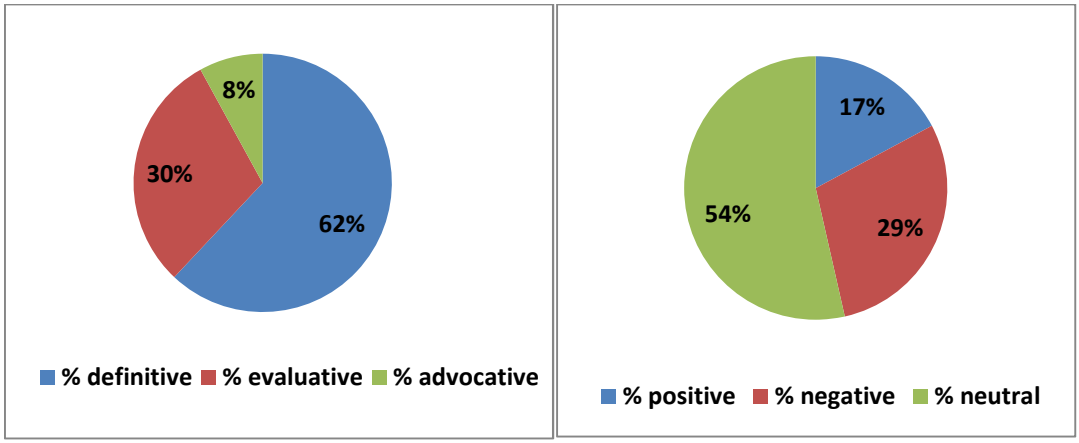
Figure 5 - General tendencies: Evaluation of Actors and their Justifications

Proponents of the scanners' implementation are the same in each country and are labelled under the categories of 'Institutions', 'Transport Security Agency' and 'Politicians', while 'Experts', 'Passengers' and 'Journalists' tend to express a more negative opinion on the topic by pointing to the concerning aspects of the scanning technology. Depending on the different national context, some peaks were identified in the actors' salience: the American case shows a higher heterogeneity of actors, meaning that the debate is conducted from different perspectives and several points of view rather than being the object of debate solely by a unique group in the society. In Italy, the 'Politicians' group is the main actor, indicating a much politicised issue, and in the UK the 'Advocacy Groups/Civil Society' category is the most salient.

The data collected on the direction of argumentation proved that, with few exceptions, the debate on the 3D Body Scanner is conducted among the European countries as a reaction to their implementation in the US and that the topic has not undergone much development. Most of the discussion is expressed through neutral and definitive statements, meaning that the topic is recognised as an external event that is considered mainly from a general and abstract perspective. The opinion expressed by the national media tended slightly toward a negative evaluation (see Figure 6).

[6] Among the various concerns, opponents to the scanners warn against the increased risk of cancer potentially posed by the radiation released during the process of scanning. Newspapers cited the experts who claimed that the amount of radiation was very small.

The origin of the actors supported the evidence that the debate is mostly reported as international news, rather than being a domestic issue within the countries. The only exception again is the US, where the coded actors were mainly Americans.



Source: SECONOMICS ISASCR

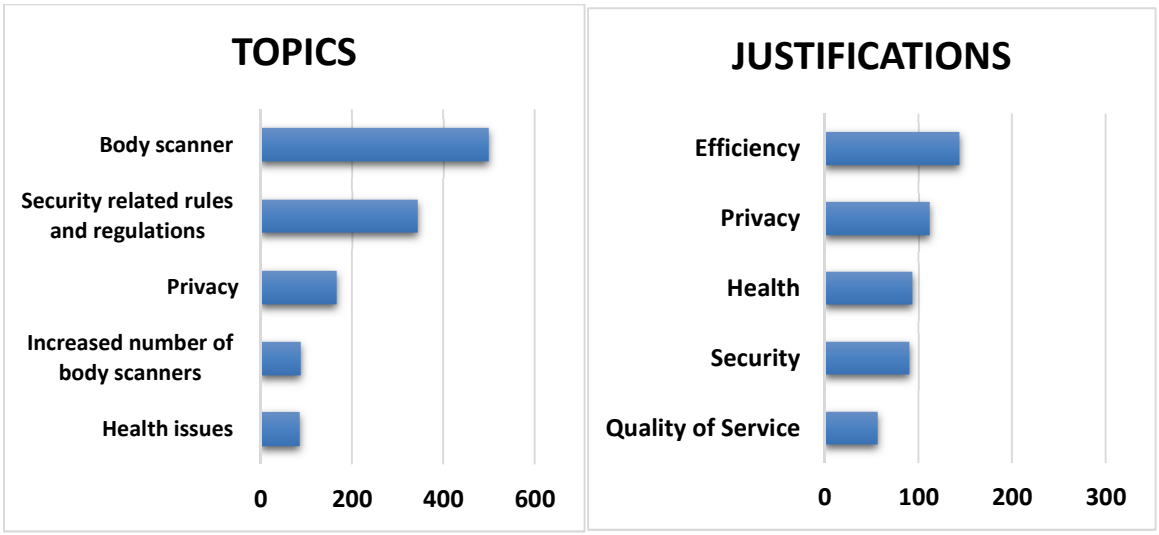
Figure 6 - Argumentative strategies and direction of argumentation in the 3D body scanner debate

The prevailing topic was the 'body scanner' itself (see Figure 7), which was particularly salient in the US and the UK. The second most salient topic was 'security related issues' which prevailed particularly in the US, the UK, and Spain. Newspapers often focused on installations of scanners and described the process of scanning. US newspapers also discussed the alternative security rules and measurements such as thermal cameras, metal detectors, tiered screening, or the usage of specially trained dogs capable of detecting drugs, weapons, and explosives.

Regarding privacy, the fear of potential misuse of the scanner images and the problem of data storage were mentioned. Similar concerns also appeared in articles that dealt with CCTV cameras. Issues of 'privacy' and the misuse of scanner pictures were connected with passengers' rights, dignity, and even with sexual harassment as the scanners originally revealed the naked bodies of passengers.

Another relevant aspect observed here, especially from new EU member states' perspectives (Slovakia, Poland, and the Czech Republic), is the lack of common and shared EU directives on the purchase and installation of the 3D body scanners: attempts to regulate the use of the device at an EU level and to provide international policy guidelines are considered to be of fundamental importance in the governments' decisions. Although the installation of the 3D body scanners remained under the powers of national legislators in EU member states, newspapers called for some kind of regulation, such as common privacy policy procedures, or regulation of the health threats posed by the device.

The American and German press also highlighted the aspect of business related to the air travel sector, both criticising the high expenditures needed for the purchase of the scanners and referring to the satisfaction of travellers. In this argument, passengers were not only citizens to protect but also consumers whose satisfaction (and thus future intent to travel by air) was important. In this respect, some passengers complained about the long and tiring queues at the security check points, the rude behaviour of the security staff and sometimes the humiliating security inspections that decreased the comfort of travelling.

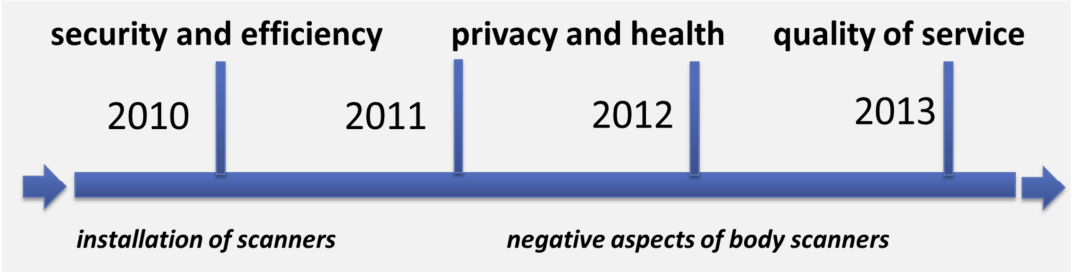


Source: SECONOMICS ISASCR

Figure 7 - Comparative assessment of salience by main topics and justifications related to 3D Body Scanners

The debate surrounding the implementation of the 3D body scanners changed rapidly over time (see Figure 8) and was closely connected with the national and international context in the observed countries, particularly in the US.

All the countries under consideration covered the failed terrorist attempt on the flight from Amsterdam to Detroit on 25th December 2009. Soon thereafter, newspapers reported on the installation of an increased number of new scanners in airports and justified this implementation with the need for higher and more efficient security measures. In the first year, 'Efficiency' was the most salient justification among all countries, and it was very often connected with the topic 'Security Rules and Regulations.' During 2011, new topics and especially new justifications started to appear in newspapers in many countries. These mainly pointed toward the negative aspects of the scanners' implementation, including the consequences on 'Privacy', 'Health' and the 'Quality of Service' (see Figure 8).



Source: SECONOMICS ISASCR

Figure 8 - Timeline of development of topics and justifications

In conclusion, this research dealt with the media's recent public discussion on 3D body scanners, focusing on the arguments and the justifications claimed by supporters and opponents, with a brief look at the main topics related to the scanners. This study provided evidence that in the US the debate is more lively and heterogeneous, motivated by a reaction to recently attempted terrorist attacks.

Summarising the results, the media coverage and public opinion's perception of the 3D body scanners were significantly influenced by two important factors. Firstly, the implementation of the device in airports affected the salience of the topic in the newspapers. As previously mentioned, the US, the UK, Germany and Italy developed a quite lively and articulated debate, while in Mexico, Poland, the Czech Republic and Slovakia where scanners have not yet been installed, the media mostly reflected and reported on the topic as an external problem which was not of particular interest to the general public. Secondly, previous experience with terrorist attacks is a factor strongly affecting security perception and the security related policies. Some countries decided to install 3D body scanners after the failed terrorist attempt on the flight from Amsterdam to Detroit on 25 December 2009, starting from the US where this 3D technology has currently become a standard procedure in aviation security protocols.

3.3 Stuxnet in printed media and security expert blogs

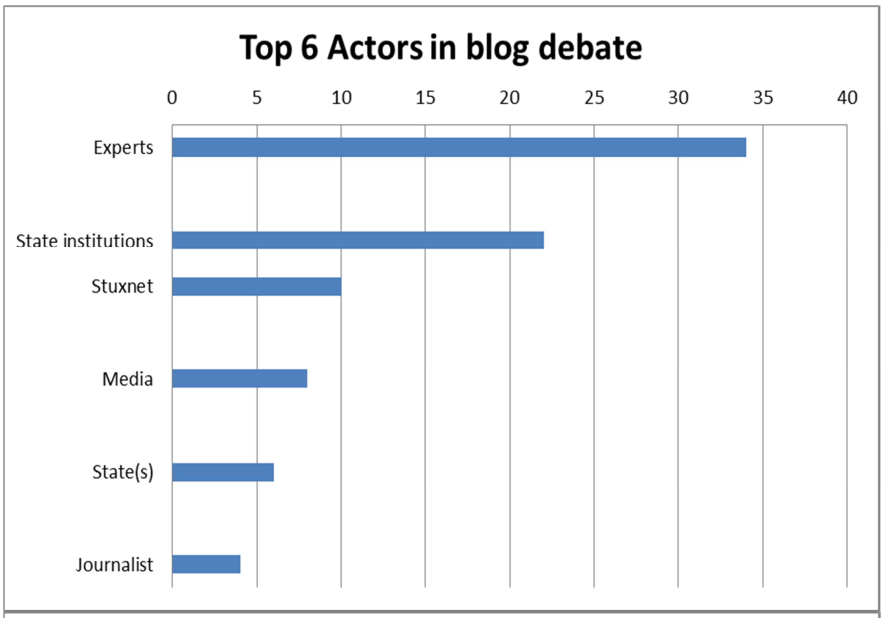
This chapter compares and combines the findings of a discourse analysis of two media arenas covering the topic of Stuxnet: mainstream media (targeting the general public) and security expert blogs (focusing on experts). In the SECONOMICS media analysis, Stuxnet was selected as a transnationally salient topic in the area of critical infrastructure to the public debate. While the mainstream media reflected shared beliefs, preferences, values and norms in the domestic and transnational arena, expert blogs are here assumed to reflect the latest developments in international security-related affairs connected to the particular topic of our study.

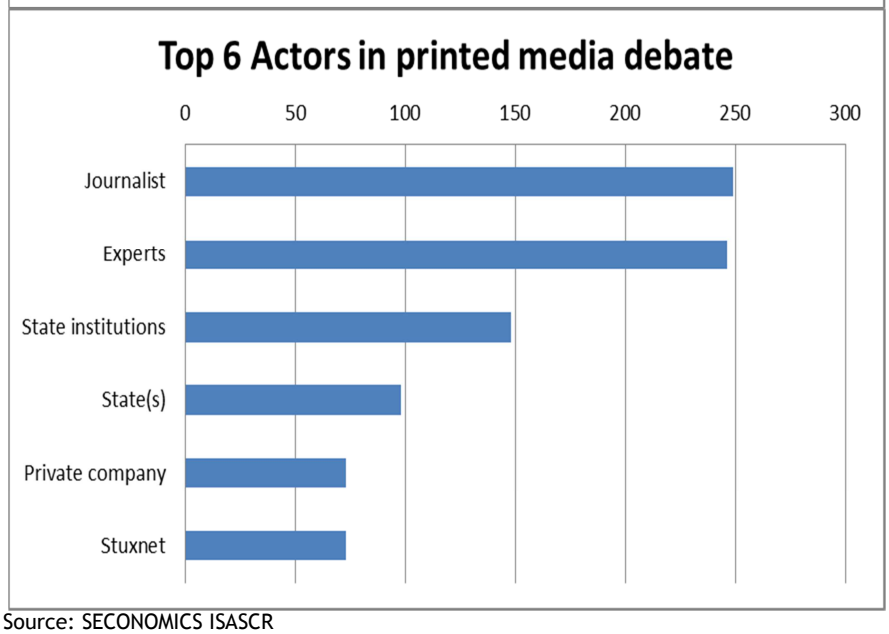
Compared to the other two SECONOMICS security topics (CCTV cameras and 3D body scanners), Stuxnet is not a technology directly affecting the lives of common people. Neither it is meant to increase the security of individuals. On the contrary, it is a weapon developed to harm critical infrastructure. As such, Stuxnet has great

implications for geopolitical stability, international law and security. Although this makes cyber security a global problem to be dealt with solely on the level of the international community, i.e. the European Union and particular nation-states, there are undoubtedly important impacts on the security of individuals as well; consider the numerous threats in the cyber world which ordinary people can face on a daily basis. Nevertheless, the prevailing content of the media debate analysed was rather descriptive and purely informative, containing no efforts for analysis or justifications. This was also surprisingly true for part of our sample of the expert blogs debate.

On this level, the media simply presented information on the Stuxnet attack on Iranian uranium enrichment facilities, tried to explain Stuxnet and speculated about the origin of the malware. Fortunately, we were able to also identify more in-depth, analytical articles handling the topic from more global point of view, mostly coming from the US and Germany. Such articles focused on wider and mostly negative consequences of the Stuxnet attack for international security, fear of possible counterattack and further diffusion and escalation of cyber-attacks in general. The American debate in particular also included statements from Stuxnet proponents. The most salient part of the expert blog debate accentuated very similar topics as this latter 'global' perspective in printed media, though some topics were approached from a slightly different perspective. Most importantly in this respect, the potential cyber war threat was called into question frequently.

The newspapers and expert blogs debate was highly comparable also in terms of actors involved, with 'experts' and 'state' (institutions) representatives ranking highest (see Figure 9). In both cases, the US was the leading country concerning the actors' origin.

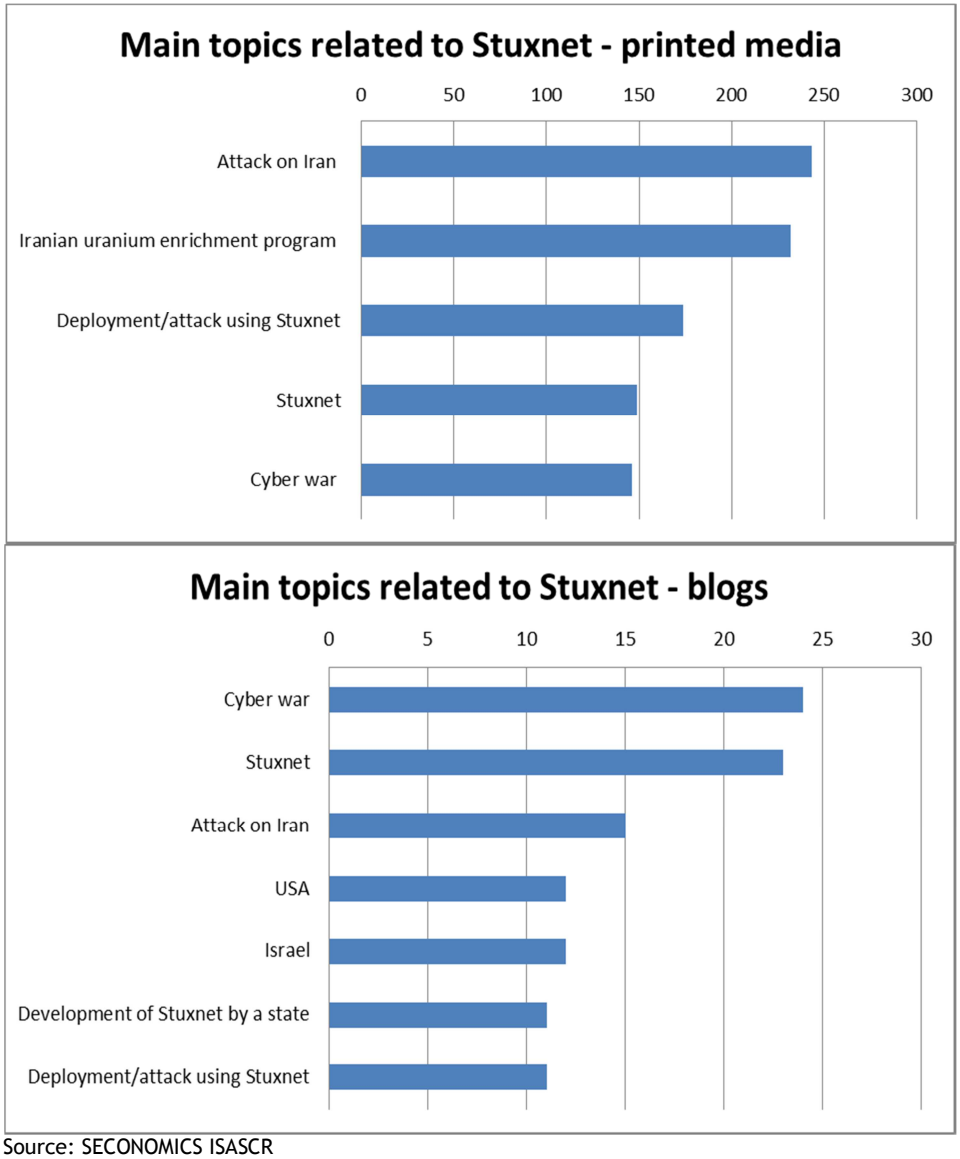




Source: SECONOMICS ISASCR

Figure 9 - Comparison of actors present in blogs and printed media (in N)

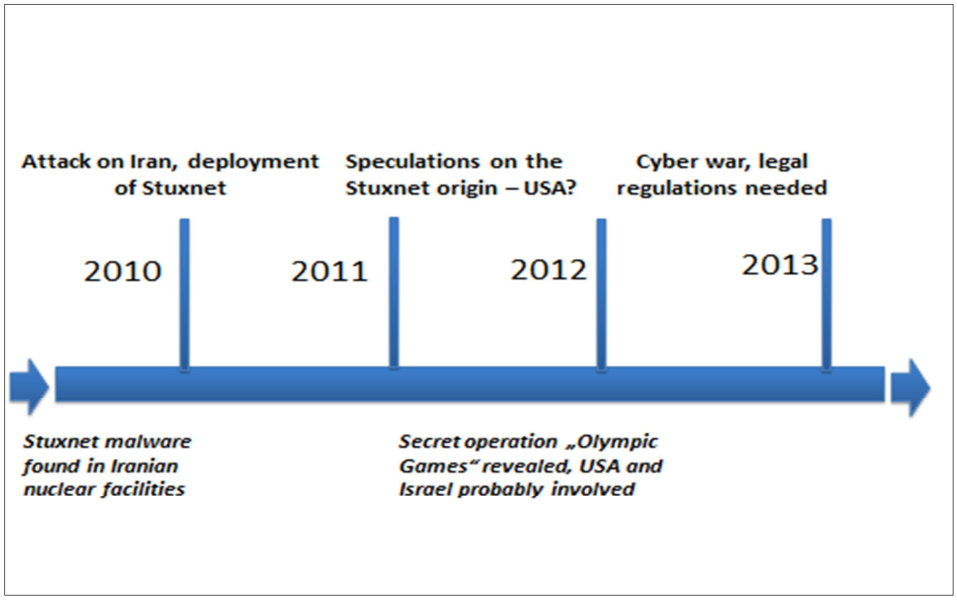
Generally, bias and pragmatism were features of the most salient part of the expert blog debate. However, the whole analysed debate on Stuxnet both in printed media in selected countries and selected security expert blogs can be regarded as one thread, with a descriptive perspective on one hand and a more in-depth global perspective on the other. This latter perspective makes up the most salient core of the debate, though not the most dominant. There were no major differences found between expert security blogs and printed media concerning this part, except a slightly different point of view on certain issues within the expert blog community stemming from its dissimilar target audience.



Source: SECONOMICS ISASCR

Figure 10 - Main topics related to Stuxnet in blogs and printed media

The debate began with informative and non-evaluative articles covering the attack on an Iranian uranium enrichment facility in Nataz (see Figure 10). After that, speculations increased regarding the origin of the malicious software. Since the discovery of the probable involvement of the US and Israel in the 2012 secret operation 'Olympic Games', which was responsible for the attack, the debate pointed to the US and its president. Later on, the debate gradually moved to a more abstract level, discussing cyber weapons in today's world and their role in potential cyber war as well as the need for regulations and protection against possible threats (see Figure 11).



Source: SECONOMICS ISASCR

Figure 11 - Timeline of development of topics and justifications

This analysis highlights that Stuxnet is not a technology directly affecting the lives of common people, such as CCTV cameras or 3D body scanners which are meant to increase security of individuals. Due to the seemingly distant character of the topic, the prevailing content of the media debate we analysed concerning Stuxnet was descriptive and purely informative, containing no efforts for analysis or justification. This was also surprisingly true for part of our sample of the expert blogs debate. On this level, the media simply presented information on the Stuxnet attack on the Iranian uranium enrichment facilities, tried to explain Stuxnet and speculated about the origin of the malware.

The most salient part of the expert blog debate highlighted very similar topics to this latter 'global' perspective in printed media. However, some topics were approached from a slightly different perspective. In this respect, potential cyber war threat was called into question frequently and we generally saw appeals for a new legal and technical framework concerning cyber security.

4. Comparative chapters

This part combines the results and findings of the three particular case studies with media results and presents multidisciplinary outcomes. Security has been defined as a subjective phenomenon that changes within society. Information on people's understanding of security issues (e. g. crime, terrorism, natural or man-made disasters), their perception of security as well as the relevant facts about the risks and dangers they face and perceive may vary according to the level of assessment, be it public or personal (individual). Furthermore, people's feelings of insecurity and their perception of the importance of security can be different in demographically diverse groups. People who are amongst the best protected and most secure in a society are likely to have much higher expectations of security than poorer, less protected people.

4.1 Beliefs on quality and value of security measures in air transport

We analysed data from an online survey administered by Deep Blue Srl (DBL). A questionnaire was designed based on the Istanbul Ataturk International Airport passenger survey conducted by Anadolu University. Since some of the questions were not appropriate for an online survey, we used a reduced and adapted version of the full passenger survey. In the survey, we collected 256 usable questionnaires (from a total of 287 questionnaires).

During the analysis, we were particularly interested in two topics: 1) the relationship between passenger perceptions on the effectiveness and the disturbance of specific security measures and 2) the factors affecting a passenger's intention to reuse air-travel.

For the first topic, we analysed (using logistic regression) the relationships between a) *believing that a security measure is useful and effective* (versus not), and b) *considering the same measure disturbing* (versus not) for the six security procedures considered in the survey (*CCTV monitoring, hand search, walk through metal detector, x-ray screening, interaction with security personnel, and full body screening*). The results showed that if a person considers a given measure effective, then it is less probable that s/he is also disturbed by that measure. This relationship was found for each of the measures considered.

We also analysed the relationships between believing that each measure is effective or disturbing and socio-demographic factors, which were also included in the survey (*sex, age, religion, reason for travelling, frequency of travel, and recency of travel*). For two security measures, we found a relationship between considering the measure disturbing and *traveling for business*. Those who reported to usually travel for business are less likely to be disturbed by walking through a metal detector and more likely to be disturbed by interactions with security personnel than those who did not report business as a usual reason for travelling.

We also found a relationship between the religion of the respondents and their perception of the effectiveness or disturbance of some of the security measures. We found that the probability of considering CCTV and x-ray screening disturbing is higher for atheists than for Christians. Moreover, relative to Christians, those who reported to have a different religion have a lower probability of considering walking through a metal detector effective and a higher probability of considering interactions with security personnel disturbing.

As for the second topic, using a structural equation model we investigated which factors affect a passenger's intention to reuse air-travel in the future (see the figure 12. below). In particular, we analysed how a passenger's intent is affected by 1) perceived quality, measured by effectiveness of various security measures, 2) perceived value, measured by belief on the effectiveness and efficiency of general security procedures, and 3) perceived equity, measured by the degree to which the passenger felt s/he has been treated fairly and rightly.

We found that while the perceived quality itself does not directly influence intentions to travel by air, it has an indirect effect (via the perceived value) on air-travel intentions. The perceived value of security procedures is enhanced by higher perception of quality, and affects air-travel intention positively (i.e., higher perceived quality → higher perceived value → higher air-travel intentions). Another important finding was the role of perceived equity. We identified that perceived equity, conceptualised broadly as different treatment due to passengers' nationality, has a positive indirect effect on the air-travel intention through perceived value (i.e., higher perceived equity → higher perceived value → higher air-travel intentions).

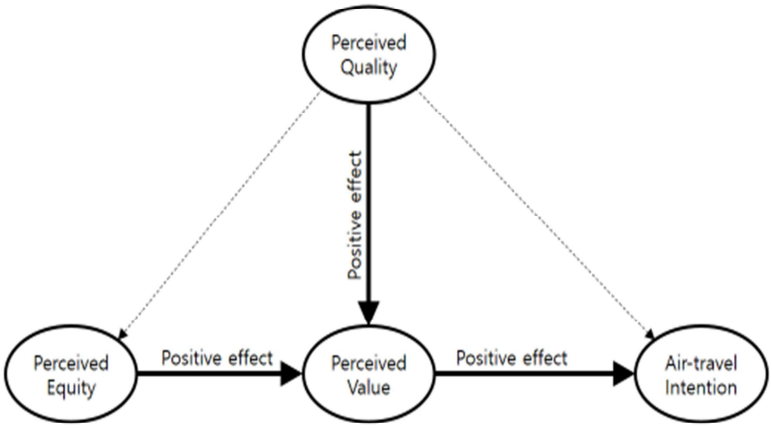


Figure 12- Structural Equation Model: A passenger's intention to reuse air-travel.

4.2 Acceptance of Security Measures in Urban Public Transport

The study of the salience of security measures in urban public transport yields highly innovative findings based on a combination of qualitative and quantitative data (qualitative comparative media analysis of the SECONOMICS Media Corpus) and industry data (Transports Metropolitans de Barcelona - TMB) macro data, security incidents, and customer complains) (for details see D4.3. and D3.4.) which were merged into a critical salience index. The comparison of the findings of the TMB case study and the subsequent validation process of the social model with urban public transport stakeholders highlighted that satisfaction with and salience of security issues has the potential to directly and indirectly influence costs of security.

Our research established that there are inherent differences in salience caused by cultural differences as well as by past exposure to security related events (e.g. terrorist attacks). Both of these facts were prominently present in the TMB case study. Unlike in other countries, CCTV camera systems, which are the dominant issue in Spain as a whole as well as in Catalonia, were uncontroversial and widely accepted. In their study of Spanish and Catalan media, Pereira-Puga and Hronešová (2013) have shown an almost complete absence of critical voices – due to its extent, this is unique in our sample and possibly hints towards an exclusion of critical voices from Spanish and Catalan newspapers in favour of state institutions.

The dominance of these actors such as the Catalonian data protection agency, the Madrid-based commission of surveillance and city councils often quoted by journalists, hints towards effective communication channels between media and state actors. In effect, the dominant discourse on CCTV cameras is that of an effective measure against petty crime and criminality in general. The technology is seen uncritically and its proliferation in the public space is welcomed.

Examination of the critical salience index indicated a very low negative salience of the three issues in question (fare evasion, uncivic behaviour (e.g. vandalism) and ticket inspectors' behaviour). In D4.3 and D3.4, we have shown in our case study that the critical salience of security measures was influenced by macro societal factors – prolonged economic crisis in Spain contributed to a growing tolerance of fare evasion and uncivic behaviour. This may possibly be seen as a rejection and a protest against the authority of the state whose handling of the crisis was perceived ambivalently. Specific factors such as growth in ticket price and training of ticket inspectors led to increased effectiveness in control of fare evasion. The more effective the ticket inspectors were, the more critical the customers were to their behaviour – in the eyes of some passengers, traveling without a ticket was justified, particularly if the fare evader was unemployed.

The validation of the social model in the domain of urban public transport emphasised the need for and importance of considering social factors in addressing security challenges both domestic (as exemplified above in the case study of Spain in a time of economic crisis) and those of globalisation and growing diversity. Security in urban public transport must consider and address the growing diversity of passengers,

particularly in regard to the communication and training of security personnel. Another dominant aspect during the validation activities was the need for comprehensive solutions to security issues. An important point raised by stakeholders was the need for security coordination within the various units of public transport providers - between different means of public transport (e.g. effective implementation of security measures in a metro can shift the security issue to public busses and vice versa), between public transport providers and security forces (i.e. the police), and pan-European coordination of both public transport providers and security forces (i.e. the police).

With regard to petty crime, the validation activities both in Barcelona (2013) and Brussels (2014) drew attention to the fact that freedom of movement within Europe is conductive to the fluid movement of organised crime groups. In particular, pickpockets are not isolated individuals but rather members of organised groups moving within Europe, adapting to the domestic context of a given country (tourist season, economic development of the country, legal and regulatory framework – for example the distinction between criminal offense and crime). The answer to this challenge, in accordance with the underlining European principles of freedom of movement and Europe without borders, is the need for increased pan-European coordination and possibly the establishment of a special taskforce focused on organised petty crime groups.

4.3 Acceptance of security measures in Critical National Infrastructure (CNI)

In regard to the salience of Critical National Infrastructures (CNI) security, SECONOMICS research highlights that both citizens and stakeholders largely underestimate the salience of security issues in said domain (D4.3, D4.4, D2.4). Furthermore, validation in the CNI domain has shown that salience and satisfaction of security issues have the potential to directly and indirectly influence costs of security (both in financial terms – as costs of implementation and in non-financial terms as acceptance of the measures by the public).

In particular, we found that there are inherent differences in salience caused by cultural differences as well as by past exposure to security related events (e.g. terrorist attacks). The cyber security domain of CNI, Internet literacy and online security awareness are key intervening factors that significantly affect the feeling of security in the online public sphere and online public spaces. In terms of the future and emerging threats, the manipulation of wholesale energy markets and IT infiltration of operational technology used to control CNI are of growing importance. Externalities include fraud and other antisocial behaviour.

On one hand national security is highly relevant, while on the other hand are the issues of freedom of speech and the protection of whistle-blowers. The need for redress in the policy domain is best substantiated by the argument shared by some policy-makers that the provision of advisory information by governments and the use of voluntary standards would be the best choice on the European level.

Assurance and reliability of information for future and emerging CNI threats and appropriate dissemination of sensitive information are key challenges. The ways to mitigate some of the issues outlined above are ensuring that issues of citizens' satisfaction are acknowledged and incorporated in allocation of resources, in the training of security personnel, and especially in the communication strategies of security stakeholders.

4.3.1 Future and emerging threats: cyber-crime

During the late 1970s and 1980s, specific data networks enabling customers to exchange messages and data began to appear. At the beginning, these were operated by very large computer and telecommunication companies, but financial services providers were early adopters of the new technology. This brought a risk of fraud, in terms of unauthorised access to an official computer terminal. Unauthorised access to networks was extremely technically and physically difficult, making such attacks almost unheard of. With the spread of personal computers in the late 1980s, we saw the emergence of recreational hackers. Among their activities were the first instances of malicious software, transmitted via floppy discs (Sommer and Brown 2011). By that time, the first successful breaks into corporate and government computers also occurred. With the wider public emergence of the Internet in the 1990s, risks grew rapidly. The main reasons were greater connectivity that provided a vector for criminal activity, considerable opportunity for anonymity, and speeding up the processes by which unsophisticated users could be misled and exploited (Sommer and Brown 2011).

Simultaneously, organisations have become much more dependent on their technology infrastructures. One of the systems worth mentioning are the so called Supervisory Control and Data Acquisition Systems (SCADA). Since 1960, these systems have been increasingly used to monitor and control utility services such as electricity, gas, water and oil. Generally, these computer systems monitor and control physical operations. In July 2010 it became apparent that one widely deployed SCADA device manufactured by Siemens had a hard coded default password, making it particularly vulnerable to attack. Just such an attack, Stuxnet, appeared shortly thereafter. The potential of cyber-attacks to be a significant threat to critical infrastructure has been discussed over the last 15 years (Collins and McCombie 2012). The first malware attack can be dated back to 1988 and others followed, with 2007 and 2008 attacks against Estonian and Georgian governmental and banking networks being the most recent and serious. In 2010, the potential to attack critical infrastructure systems was finally realised with the advent of the malware Stuxnet. Stuxnet, unlike the malware that came before, is highly targeted and designed with a real-world outcome in mind, specifically to sabotage the Iranian nuclear programme (Collins and Mc Combie 2012). In May 2010, the malware was discovered by an antivirus company Virusblokada, based in Minsk, Belarus.

There is an increasing tendency for firms engaged in large scale manufacturing and critical infrastructures to integrate both core and corporate assets. The primary reasons for this are primarily driven by the need for flexible operating capacity that can be

monitored in the same way as standard business assets. A typical and current example is the use of data historians, with SCADA systems, which sit in the corporate IT environments. They allow the business to develop for automated, efficient and cost effective business processes to be used in the core CNI environment.

A secondary reason is that for regulated industries there can be significant cost implications for switching processes to unregulated corporate network assets. To this end, the numbers of industrial control systems (ICS) such as the aforementioned SCADA type have Internet facing connectivity. Historically, many of the ICS/SCADA systems are legacy and hence are not designed to detect or repel malicious activity. This traditionally has been less of an issue, as the ICS/SCADA systems have not had any Internet facing components. However, several sophisticated malware technologies have been deployed, most likely by state actors that have exploited USB sticks as a means of overcoming these gaps.

4.3.2 Stuxnet – a milestone in cyber-security

In September 2010, the Bushehr nuclear power plant in Iran was believed to have been infected by Stuxnet. Stuxnet showed a level of sophistication never seen before and was indicative of professional malware writers, not standard typical hackers or cyber-criminals (Williams 2011). It was also the first time when a computer worm caused physical destruction in the real world by damaging nuclear facilities.

More importantly, the Stuxnet attack generated serious implications within strategic and political contexts. It has shown that, compared to traditional military means, cyberspace carries less cost and risk in use against enemies and proved that cyber terrorism is now a credible threat to nation-states. The threat has now moved beyond conventional surface targets to critical infrastructures, which are heavily dependent upon computer systems. The unprecedented scope and efficiency of Stuxnet consequently managed to shake public views of cyber-security (Guasti and Mansfeldova 2014).

4.3.3 Pan-European coordination

Future and emerging threats in the CNI domain may come jointly from the re-engineering of complex malware such as Stuxnet and Flame and software generated in advance for use in information gathering and in the case of Stuxnet offensive actions. Other threats may emerge from the general exposure of critical infrastructure to accidental interaction with malware not specifically designed to exploit or injure CNI systems. The major dangers stem from the highly integrated nature of future projected CNI infrastructures as smart grids (on the transmission side) and smart metering (on the consumer side). Systematic flaws in commonly used information assets (such as IT operating systems and firmware used in many devices such as Smart Meters) may result in systematic and widespread damages to the CNI system as a whole. These concerns have been outlined extensively in many of the blog posts contained in the CNI data set.

In the United States, the National Institute of Standards and Technology (NIST) platform is presented by many of the blog posts as an approach to ensure integration across various different industries in order to guarantee a degree of standardisation and security. From the EU perspective, the Network and Information Security (NIS) Platform is proposed to be a similar mechanism to the NIST, focusing on sharing incident data on malware between industrial communities (such as CNI operators) and providing a variety of emergency response techniques and advice. However, the NIS platform currently lacks credibility and maturity in comparison to NIST as NIST have built their knowledge and leadership in security over a number of decades.

5. Conclusions. Future and emerging threats.

This chapter summarises findings and presents an answer to the question posed in the title of this deliverable about the price of security in contemporary society.

5.1. Security and the media

Based on the examination of the role of the media in political communication, our research confirms that on transnationally salient security issues, the media fulfil two roles – that of an information transmitter and of a public opinion maker (cf. McNair 2011). Our case studies include cyber-terrorism as an example of risk and 3D scanners and CCTV cameras as examples of security measures, although, as mentioned above, some media outlets framed Stuxnet as a security measure. The main factors shaping how the media report on security threats and security measures are past experience with a particular security threat and the probability of the country being targeted in the future (cf. Beck 2000, 2002). These factors account for the main differences in the extent of coverage dedicated to the issue in different domestic media.

The media debates in the studied countries each prioritised a specific aspect of national security in reaction to the effects of both global events (i.e. terrorist attacks) and domestic developments (economic and political). Countries that are generally more active on the international scene and/or have had a previous experience with domestic and international terrorism are generally more exposed to (and hence concerned about) potential terrorist attacks. In these countries (the UK, the US, Spain, and Germany) security measures are high on the policy agenda, as demonstrated by the prioritisation of body scanners in airport security and intensified CCTV camera use in counter-terrorism. In countries with no real danger of a terrorist attack by (international/national) extremist groups (Poland, the Czech Republic, Slovakia), there is a low policy interest in advanced and costly security devices such as body scanners at airports and CCTV cameras and they are seen positively as a crime prevention measure.

Still, developments in 2013 show that acceptance of security measures depends on the perception of their use as both legal and legitimate, regulated by laws that maintain appropriate scrutiny. Hence the attempts of countries to justify installation of CCTV cameras as a crime prevention measure whilst seeking to enhance counter-terrorism can actually backfire and deteriorate public trust, as seen in the UK case study (Hronesova, Guasti, and Caulfield 2014).

However, it is not only experience with terrorist attempts and threats that determines the attention paid by the media to different security measures and tools. It is also the nature of these measures and tools and the extent of their applicability to the domestic context. This also influences the composition of actors who communicate with the public through printed media. In the case of CCTV cameras, journalists dominated the debate; they were the most important actors in seven countries. Stuxnet represents a special case among the three selected topics, as it does not directly affect individual security, but rather national security. It is also a highly complex technical issue. Hence

mainly experts spoke about Stuxnet. In the debate surrounding 3D body scanners, many different actors were involved. Here, the US was indisputably the leading country in the debate and the remaining nine countries in the sample were rather reactive to the US in terms of actors, patterns of interaction, topics, and justifications.

As highlighted in chapter 3.1, there are two opposing trends in regard to CCTV cameras. In Spain as well as in the new EU member states (most dominantly in Poland), CCTV cameras are viewed uncritically as a symbol of progress and modernisation and the issues of privacy and data storage are mostly marginal. On the contrary, in the second trend present mostly in old EU member states (most predominantly in Germany and the UK) the discourse of CCTV cameras was dominated by the potential for security measures to restrict privacy and personal freedoms.

Furthermore, the acceptance of public space monitoring is rather nuanced – while the monitoring of streets and public transport enjoys a rather positive salience, the salience of CCTV monitoring in schools, hospitals, work places, prisons etc. is more critical. This underlines the need for a more differentiated view of the public sphere in policy-making processes. Last but not least, the salience and acceptance of security measures displays dynamic development, as it is conditioned by inherent cultural differences, past experience with acts of terrorism (and in the case of CCTV past and present above average degrees of organised crime), and by the plurality of media debates (degree of inclusiveness, in particular the presence of experts, advocacy groups and civil society).

Events such as acts of terrorism (the Boston marathon bombing in 2013, the terrorist attempt in Bonn in 2013) can cause a dramatic shift in the salience of a security measure, most interestingly in a shift from negative to positive salience (as in the case of CCTV in both the US and Germany). However, after terrorist attacks the media are usually dominated by voices of actors favouring the monitoring of public spaces. After the initial shock subsides and the plurality of media debate returns to its initial level, the salience of the given security measure returns (almost) back to its initial standpoint. Hence while dramatic events such as acts of terrorism have the power to significantly influence public opinion, their impact is not as lasting as that of cultural attitudes and media landscape.

5.2. Salience of Security in SECONOMICS Case Studies

In our salience analysis of airport security, we found that acceptance of security measures in the context of airports is connected with the perception of the given measure's effectiveness. Furthermore, the analysis shows that the perceived values of security procedures are enhanced by higher perception of quality and affect intent to travel by air. Furthermore, we established an indirect but positive relationship between perceived equity (conceptualized broadly as different treatment due to passengers' nationalities) and intention to travel.

The study of the salience of security measures in urban public transport also yields highly innovative findings. Examination of the critical salience index indicated very low

negative salience of the three issues in question (fare evasion, uncivic behaviour e.g. vandalism, and ticket inspectors' behaviour). The validation of the social model in the urban public transport domain emphasised the need for and importance of considering social factors in addressing security challenges, both domestic and those of globalisation and growing diversity. Another dominant aspect during the validation activities was the need for comprehensive solutions to security issues.

Security coordination was an important point raised by stakeholders. Coordination was called for within the various units of the public transport provider, between different means of public transport (for example, effective implementation of security measures in a metro can shift the security issue to public busses and vice versa), between public transport providers and security forces (i.e. the police), as well as pan-European coordination of both public transport providers and of security forces (i.e. the police).

In regard to the salience of CNI security, SECONOMICS research highlights that both citizens and stakeholders largely underestimate the salience of security issues in the domain (D4.3., D4.4., D2.4). Furthermore, the validation in the CNI domain shows that salience and satisfaction of security issues have the potential to directly and indirectly influence costs of security.

Assurance and reliability of information for future and emerging CNI threats and appropriate dissemination of sensitive information are key challenges. The ways to mitigate some of the issues outlined above are ensuring that the satisfaction of citizens is acknowledged and incorporated in the allocation of resources, in the training of security personnel, and in substantially addressing the communication strategies of security stakeholders.

Future and emerging threats in the CNI domain may come jointly from the re-engineering of complex malware such as Stuxnet and Flame as well as software generated in advance for use in information gathering and (in the case of Stuxnet) offensive actions. Other threats may emerge from the general exposure of critical infrastructure to accidental interaction with malware not specifically designed to exploit or injure CNI systems. The major dangers stem from the highly integrated nature of future projected CNI infrastructures as smart grids (on the transmission side) and smart metering (on the consumer side). Systematic flaws in commonly used information assets (such as IT operating systems and firmware used in many devices like Smart Meters) may result in systematic and widespread damages to the CNI system as a whole. These concerns have been outlined extensively in many of the blog posts contained in the CNI data set.

5.3. The price of security

In the introduction, we highlighted two features important to modern democracy – security and satisfaction. In recent months, however, it has become more evident than ever before that these concepts are closely connected. As highlighted above in part 2.1., the publication of information about wide-reaching surveillance in many Western

countries, the reaction of the public to the information, the reaction of governments and the actions taken by these governments to severely prosecute whistle-blowers for 'threatening national security' all demonstrate that more security does not necessarily make for a happier society. The main reason is that happiness is not just connected to the absence of fear and a feeling of safety - it is also connected to the absence of far-reaching security measures that infringe on privacy and feelings of freedom. In addition to shedding light on the tension that exists between security and freedom and the costs of security in terms of privacy, recent whistle-blower cases such as Manning and Snowden have also highlighted the role of the media as an outlet for whistle-blowers and as watchdogs of freedom, privacy, and civil liberties.

Since Thomas Hobbes' Leviathan, it has been evident that safety and security, two essential features of the social contract, have their price; that freedom, both personal and that of a society, is a defining feature of legitimate government, and that governments are seen as legitimate if they are able to resolve the tension between safety and freedom to the general satisfaction of the people. The dilemma of our times, for governments, for the media, and for individual citizens, is thus the question of how much safety we want and at what price. The answers to this question differ sharply according to the political orientation of the speaker. However, the media play a critical role as an arena in which information is made available to the public, multiple claims and justifications are presented and discussed, and essentially opinions are formed.

This deliverable highlights that the balance of security and freedom is the crucial task of contemporary governments, and that the role of the critical media as a platform for public political discourse and as a guardian of freedoms is gaining considerable importance.

REFERENCES

Altheide, D. 1997. "The news media, the problem frame and the production of fear." *Sociological Quaterly* 38(4):647-668.

Beck, U. 1992. *Risk Society: Towards a New Modernity*. New Delhi: Sage.

Beck, U. 2000. *Risk society revisited: theory, politics and research programmes. The risk society and beyond: Critical issues for social theory*. London: Sage.

Beck, U. 2002. "The Terrorist Threat. World Risk Society Revisited." In: *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*. http://www.seconomicsproject.eu/downloads.

Belakova, 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*. http://www.seconomicsproject.eu/downloads.

Collins, S. and S. McCombie. 2012. "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications." *Journal of Policing, Intelligence and Counter Terrorism* 7 (1): 80–91.

Cornish, P., D. Livingstone, D. Clemente, and C. Yorke. 2011. *Cyber Security and the UK's Critical National Infrastructure*. Chatham House.

Davis, D. W. and B. D. Silver. 2004. "Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. " *American Journal of Political Science* 48(1): 28-46.

De Gramatica, M. 2013. "Better Naked than Dead. Communicating Security. Analysis of Italian Perception of Security Related Issues." Prague SECONOMICS Discussion Papers 2013/1. http://www.seconomicsproject.eu/downloads.

Farwell, J. P., and R. Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53 (1): 23–40.

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*. http://www.seconomicsproject.eu/downloads.

Gawrecká, D., J. Hronešová, P. Vamberová, P. Guasti and Z. Mansfeldová. 2014. Comparative Analysis. Contribution to the SECONOMICS project and Prague Graduate School in Comparative Qualitative Analysis 2013. *Prague SECONOMICS Discussion Papers 2014/2*. http://www.seconomicsproject.eu/downloads.

Giddens, A. 1999. "Risk and Responsibility." *Modern Law Review* 62(1): 1-10.

Guasti, P. and Z. Mansfeldová. 2014. Paper prepared for IPSA Conference, Montreal, Quebec, Canada, 20 - 24 July 2014, Session RC43: Religion and Politics, Panel: Governance Implications of EU Integration for Post - communist States.

Guasti, P., Z. Mansfeldová, J. Hronešová, D. Gawrecká, P. Vamberová, T. Lacina, U. Turhan and A. Tedesschi. 2014. "D4.3 – Communication patterns and effective channels of communication." SECONOMICS project.

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

Holguìn-Veras, Josè, Xu Ning, Bhat Chandra, 2012. 'An assessment of the impacts of inspection times on the airline industry's market share after September 11th'. Journal of Air transport Management, 23, 17-24.

Hronesova, J., P. Guasti and T. J. Caulfield. 2014. "The Xanadu of surveillance: Report on security perceptions in the British online media." *Prague SECONOMICS Discussion Papers 2014/3*. http://www.seconomicsproject.eu/downloads.

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

Lindsay, J. R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies*, 22: 365-404. http://www.tandfonline.com/doi/pdf/10.1080/09636412.2013.816122.

Lyon, D. 2002. *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. Routledge.

Mackey, David A. 2007. 'The 'X-rated x-ray': Reconciling Fairness, Privacy and Security.' *Criminal Justice Studies* 20 (2): 149–159. [online]. Available from: http://www.tandfonline.com/doi/ref/10.1080/14786010701396889#tabModule. Accessed 10 June 2014.

Mackey, David A., Michael W. Smith. 2012. 'X-ray scanning, wiretaps, and other searches: examining college students' perceptions of the reasonableness and intrusiveness of homeland security searches.' *Criminal Justice Studies* 25 (4): 371-389. [online]. Available from: http://dx.doi.org/10.1080/1478601X.2012.728785. Accessed 16 April 2014.

Mansfeldova, Z., P. Guasti, D. Gawrecka, P. Vamberova, T. Lacina. J. Hronesova, Alessandra Tedeschi. 2014. "D4.4 – Discourses and Justification of Security and Risk." SECONOMICS project.

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

Munné, R., Pellot, M., Guasti, P., Mansfeldová, Z. and J. Cano. 2014. "D3.4 – Model Validation." SECONOMICS Project.

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

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

Rajaonah, Bako, Castelli, Juan Carlos, Ravenel Jean-Bernard, Ormont, Antoine, Cabrol, Pierre and Le Fur Gwenn, 2014. 'Acceptability of security scanners at airports.

Ruprai, R., Keay, C., Collinson, M., Pym, D., Williams, J., Guasti, P., Mansfeldová, Z. and A. Tedeschi. 2014. "D2.4 – Model Validation. National Grid Model Validation." SECONOMICS Project.

Sjöberg L. and A. Wåhlberg. 2000. "Risk perception and the media." *Journal of Risk Research* 3 (1): 31-50. http://www.dynam-it.com/lennart/pdf/rp%20and%20media.pdf.

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

Sommer, P., and I. Brown. 2011. Reducing systemic cybersecurity risk. *Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS (2011), 3*.

Tirosh, Y. and M. Birnhack. 2013."Naked in Front of the Machine: Does Airport Scanning Violate Privacy?" *Ohio State Law Journal* 74: 6.

Vamberová, P. 2013. "I"ll Be Watching You. Communitacing Security and Privacy Issues in the Mexican Press." *Prague SECONOMICS Discussion Papers 2013/4*. http://www.seconomicsproject.eu/downloads.

Williams, B. 2011. *Ethics and the Limits of Philosophy*. Taylor & Francis.