SECONOMICS

Report on Expert Blogs Analysis

Document Information

Document Number	
Document Title	Report on Expert Blogs Analysis
Version	1.0
Status	Final
Work Package	WP 4
Deliverable Type	Report
Contractual Date of Delivery	
Actual Date of Delivery	09.01.2014
Responsible Unit	ISASCR
Contributors	Tomas Lacina, ISASCR
Keyword List	CCTV, Stuxnet, Body scanners
Dissemination level	

SEVENTH FRAMEWORK PROGRAMME

Security Economics: Socio economics meets security

Table of Contents

1 Introduction

Every day, the daily news coming from various parts of world can only enforce our conviction that security issues are one of the most salient domains in contemporary societies. Moreover, in the globalized system, various conflicts, risks and other security issues naturally become global, crossing the boundaries of nation states and having a long latency period. Danger and insecurity have always been inherent to human life, especially in the form of natural disasters and the like. However, post-modern societies experience a new type of risks, which are mainly a product of human activity, such as nuclear radiation, global warming, financial crises and terrorism (Beck 1992 and Beck 2002). As Beck (1992) argues, the new risks have become a central dynamics characterizing contemporary societies and have led to transformation of the whole society and social order (Vrablikova 2012). Within this context, it seems plausible to raise questions on risk perception of individual citizen and differences in risk perception among various groups. That implies further questions concerning impacts of various risk perceptions on human behavior, political decision-making and economy. This range of issues constitutes an important part of the SECONOMICS project objective, which is a broad cross-disciplinary 7FP project, aiming to provide a socio-economic rationale to security policy making. The SECONOMICS project focuses on three key security topics: critical infrastructures, airport security and regional and urban transport. For each topic, a case study has been developed to scope important issues in security management. The scientific research of the project combines models of game theory, systems modelling, adversarial risk analysis and social policy in a unified framework. This framework will provide insight for policy makers in determining the design of effective security policy, security investment, the public acceptance of security and finally the incentive structure of individuals and organizations with respect to security (Williams and Massacci 2013).

Outcomes of quantitative secondary data analysis of existing works on risk and threats using cross-national surveys brought an important general overview of citizen’s perceptions and attitudes towards risk and security (Guasti 2013). However, the use of secondary sources appeared to have limited relevance for the SECONOMICS case studies. Consequently, there was a need to supplement these data, which was done by the means of self-created qualitative data collection from print media. The media analysis conducted in the scope of this project offered a good basis for comparative analysis concerning communication channels and communication patterns between policy makers, stakeholders and citizens in the area of security (Guasti 2013). Moreover, media have an important “agenda-setting“ effect, placing certain issues in the minds of people, including policy makers. Such an ability of mass media to direct public attention and governmental action toward specific policy concerns has been documented in many cases, e.g. in the area of risks to health and the environment (Mazur 2006, Wiegman et al. 1989). This force function of media constitutes also an important factor for relevance of media analysis in the field of security issues.

As a supplement to news analysis, four English language expert security blogs were chosen to deepen the insight into communication patterns with those inside the security expert community. The issue of blogs appears to be increasingly important as the area of new media and online journalism has been growing rapidly. With rising evidence, the internet is shown to have had reinforcing effects on information-seeking and sociability. Certain web uses contribute to civic engagement and trust, increased volunteerism, enhanced personal interactions and increased news consumption (Gil de Zuniga et al. 2009). However, this appears not to happen solely based on the migration of traditional news sources online, but it also occurs via the emergence of an interactive opinion space of personal journals or weblogs (blogs).

The aim of this study is a presentation of the findings of the expert security blogs analysis between 1st January 2010 and 31st April 2013. The main research questions here are: 1. What is the overall salience of selected topics among security bloggers? 2. How do expert blogs frame the implications of security and security technologies within our three SECONOMICS topics – Stuxnet, CCTV cameras and 3D body scanners?

Being the global source of information, the expert blog articles were naturally assumed to resonate with the latest development in international security-related affairs connected to particular topics of our study, such as airliner terrorism, cyber-attacks, criminality and surveillance of public areas.

2 Backround

2.1 Blogs, blogging

Blogs can be regarded as a part of a wider group of social media including internet forums, wikis, social blogs, social bookmarking, Facebook, Twitter and others. The common attribute of social media would be turning communication and news consumption into interactive dialogue. The research conducted among European journalists has shown that the primary use of social media by journalists is around the broader process of compiling stories, promoting them and getting feedback from the public. The research also shows that social media is also regarded as extremely useful and easy to use. The only concern that was raised was regarding the credibility of the information (Journalists and Social Media – Eurobarometer Aggregate Report, January 2012).

There is no generally agreed-upon definition of blogs. They can be referred to as online interactive journals that facilitate information exchange between users called "bloggers" and that have a particular code of writing. Topics are usually arranged in reverse chronological order and information is periodically updated by the person in charge (Gil de Zuniga et al. 2009). Blogs can function as personal diaries, technical discussion, sports commentary, celebrity gossip or political discussion sites or all of above (Drezner and Farrell 2004). Blogs distinctively incorporate links to other blogs, webpages, forums etc., thus becoming interconnected and interdependent, with some of them becoming central (Drezner and Farrell 2004). They are interactive, non-synchronous webpages, whose host uploads postings that center around a certain topic. The writing needs not to be following the standards and practices of traditional media, such as balance in viewpoints, facts-based reporting and the like (Gil de Zuniga et al. 2009).

The blogosphere has grown at an astronomical rate from numbers in thousands in year 2000 to the range of 2.1 – 4.1 million in 2003 and finally to 133 million blogs being tracked worldwide by the end of 2008 by Technorati (www.technorati.com), a blog search engine (Gil de Zuniga et al. 2009, Drezner and Farrell 2004). With rising importance, blogs are increasingly portrayed as community forums or political outlets, as opposed to the initial understanding of blogs as forms of personal self-expression. Blogs offer a pattern of active online communication with environment of user control, content richness, increased immediacy and interactivity, and provide audiences control across multiple choices (Meraz 2007). The participatory and autonomous nature of blogs has made them a central part of the new media landscape (Kraushaar 2009).

Traditional media attention to blogs has also increased dramatically. As the blogosphere has grown, a variety of institutions have adopted their form. Many opinion journals, newspapers, websites of TV news channel networks host blogs on their websites. There is also strong evidence that media elites – editors, publishers and columnists – consume political and expert blogs (Drezner and Farrell 2004), indicating connection of political and expert part of the blogosphere with the media sphere. This makes respective blogs even more relevant and influential within the general media context. Reasons for this may be that expert blogs offer specialized and detailed knowledge for wide range of issues, thus reducing the search costs for traditional journalists greatly. Furthermore, bloggers have first-mover advantages in formulating opinions. The rapidity of blogger interactions can affect mainstream media through an agenda setting effect – e.g. if a critical number of elite blogs raise a particular story, it can attract the interest of mainstream media outlets (Drezner and Farrell 2004).

2.2 Context

This section deals with the most important global international security related events, relevant to specific topics of our study.

Stuxnet computer worm was discovered in June 2010. It is speculated to have been created by United States and Israeli agencies to attack Iran's nuclear facilities. Stuxnet initially spreads via Microsoft Windows, and targets Siemens industrial control systems. While it is not the first time that hackers have targeted industrial systems, the first publicly known intentional act of cyberwarfare to be implemented, it is the first discovered malware that spies on and subverts industrial systems. Different variants of Stuxnet targeted five Iranian organizations, with the probable target widely suspected to be uranium enrichment infrastructure in Iran.

Concerning air-traffic oriented terrorism, there has been a number of airliner bombing attempts in 2000-2010, such as the case of Northwest Airlines Flight 253, which was an international passenger flight from Amsterdam, Netherlands to Detroit, United States. The flight was the target of a failed al-Qaeda bombing attempt on December 25, 2009, in which a passenger tried to set off plastic explosives sewn to his underwear. Another example would be the Russian aircraft bombings of August 2004, terrorist attacks on two domestic Russian passenger aircraft flying from Moscowian Domedovo Airport or the 2006 transatlantic aircraft plot, which was a terrorist plot to detonate liquid explosives carried on board at least 10 airliners travelling from the United Kingdom to the United States and Canada. The plot was discovered and foiled by British police before it could be carried out. These events provoked a discussion and concerns in introducing **full-body scanners**, being able to detect non-metal objects carried by passengers. Starting in 2007, full-body scanners started replacing metal detectors at airports and train stations in many countries. Some passengers and issue advocates have objected to having pictures of their naked bodies displayed to screening agents or recorded by the government. Some critics have called the imaging virtual strip searches without probable cause, and some have claimed they are illegal and violate basic human rights. In 2007, a U.S. federal appeals court ruled in a lawsuit brought by the Electronic Privacy Information Center that even the naked-picture version of the technology was a reasonable and constitutional search. In the United States, federal law requires that starting in June 2013, all full-body scanners must use a software, which replaces the picture of a nude body with the cartoon-like representation.

Referring to **CCTV cameras** and public surveillance theme, a strong discussion was called out by measures being adopted recently by United Kingdom. Based on previous testing projects (e.g. Project Laser or Project Spectrum), most motorways, main roads, town centres, ports and petrol station forecourts have been covered by CCTV camera networks using automatic number plate recognition, since March 2006. Existing traffic cameras in towns and cities are being converted to read number plates automatically as part of the new national surveillance network. The police have real-time access to all ANPR camera data. Effectively, the police (and the security services) can track any car around the country in close to real time. Although CCTV in general has public and political support in the United Kingdom, there is concern about privacy in the face of the unification of different systems and databases, such as car number plate recognition cameras, being linked to personal data. Moreover, installations of ANPR systems in certain areas, brought so much controversy, that it was later suspended. This was the case of a Project Champion, which was a project to install a network of ANPR cameras to monitor vehicles entering and leaving the two neighbourhoods of Birmingham, both of which have large Muslim communities. Its implementation was frozen in June 2010 amid allegations that the police deliberately misled councillors about its purpose, after it was revealed that it was being funded as an anti-terrorism initiative, rather than for 'reassurance and crime prevention'.

3 Methodology

3.1 Research design

In this paper, a method of qualitative textual analysis of blog posts is used as a basis for a further comparative qualitative analysis at later stage of the research. The analysis is centered on three security issues, which were studied within the SECONOMICS case studies - 3D body scanners, Stuxnet and CCTV cameras. The main research questions of this study are: What is the overall salience of selected topics among security bloggers? How do expert blogs frame the implications of security and security technologies within our three SECONOMICS topics? What is the perception of security risks among the security expert blog community? Do the questions of security dominate opposed to the issues of privacy? Is the discussion within the community prevailingly very expert and technical or rather opinion based? For comparative purposes, the analysis was limited to articles published between 1st January 2010 and 31st April 2013. The essential unit for the analysis is a “statement”, which we refer to as a part of a text (a sentence, part of a sentence or a whole paragraph). The criterion for designation of a statement is that it holds an “idea”, meaning that a statement must make sense for those who read it without the rest of the article. Also, to classify a statement, we have to be able to identify an actor making an argument about one of our selected topics. For the purpose of this study we obviously selected only the statements that included the subject of our study, the keywords of CCTV cameras, 3D body scanners or Stuxnet.

3.2 Coding

The analysis was then conducted by coding articles using *Atlas.ti7*. For each statement, codes were ascribed for seven different categories (see Table 1). While not each statement could be assigned codes for all categories, codes in categories 1 – 4 were mandatory for each statement to be included in the analysis. Each of the three topics was coded by a distinctive coding scheme. The coding schemes were designed based on pre-tests and then further amended during the training sessions at the Graduate School in Comparative Qualitative Analysis in Prague.

Table 1: Basic coding structure

Coding categories	**Coding subcategories**
Actor (1)	
Topic (2)	
Argumentation (3)	a) definitive b) evaluative c) advocative
Direction of argument (4)	a) positive

	b) negative c) neutral
Justification (5)	
(Actors') Interaction (6)	
Actor's origin (7)	

3.3 Data gathering

3.3.1 Source selection

Altogether four security expert blogs in English language were selected for the purpose of the analysis: *Bemosa* (bemosa.blogspot.com), *Roger-Wilco* (www.roger-wilco.net), *Hack in the Box – HITB* (www.HITB.org) and *The Register* (http://www.theregister.co.uk). These blogs were selected in two rounds. First, SECONOMICS experts on airport, public air transport and critical infrastructure security provided a list of recommended blogs. The second selection criteria were based on readers' turnout and relevance to objectives of the study.

Bemosa defines itself as an Airport Security Monitor. It is the corporate blog of Kirschenbaum Consulting, which is a provider of professional security consulting services to airports, transport authorities, governments, security companies and other high-risk organizations. The blog is written by Professor of ? Alan Kirschenbaum, an expert in the area of disaster and crisis management, and the formally initiator and coordinator of the EU-funded *BEMOSA* Project (www.bemosa.eu), a Europe-wide research project which developed a behavior model that describes how people make security decisions in the face of reality during normal routine and during crises. This professional blog covers the latest news, research and analysis on the impact of human factors on airport security.

Roger-Wilco is a blog dedicated to the subject of air traffic management, viewed through the eyes of the people most immediately concerned by it, air traffic controllers, pilots, engineers and managers on all levels. The content is written by and for aviation professionals with reader comments. It is structured to categories in alphabetical order, security being one of them. The blog is an initiative of BluSky Services, which is a private company providing consulting and service in the area of air traffic management.

Hack in the Box is a blog with the most mysterious background out of the four, as it was not easy to find information on the blog operator and its nature. After contacting directly Mr. Dhillon Andrew Kannabhiran, the CEO of the *Hack in the Box* (or *HITB*), we finally got the answer. Mr. Kannabhiran defines *HITB* as the community of organizers of the *HITB* Security Conference or *HITB*SecConf series of community-backed, not-for-profit security conferences held annually in Kuala Lumpur, Malaysia and Amsterdam, Netherlands. The main aim of *HITB*SecConf is to "enable the dissemination, discussion and sharing of deep knowledge network security information with a focus on groundbreaking attack and defense methods." *HITB*SecConf is endorsed by the Malaysian Communications and Multimedia Commission (MCMC), Malaysian National Computer Confederation (MNCC), Multimedia Development Corporation (MDeC), MSC Malaysia and the Malaysian International Chamber of Commerce and Industry (MICCI).

The Register is a British technology news and opinion website/blog founded in 1994. Situation Publishing Ltd is listed as the site's publisher. *The Register* was founded in London as originally an email newsletter called Chip Connection. In 1998 *The Register* became a daily online news source (Walsh 2007). In 2002, *The Register* expanded to have a presence in London and San Francisco, creating *The Register* USA at theregus.com. In 2003, that site moved to theregister.com. That content was later merged onto theregister.co.uk (Cullen 2003). As for readership, according to the Audit Bureau of Circulations, it was read daily by over 375,000 users in 2012 (www.abc.org.uk, retrieved 24th October 2013). In May of 2013, Alexa (a company providing commercial web traffic data) reported that the site ranked no. 4,012 in the world for its web traffic, down approximately 1,000 slots from the prior year. The content of *The Register* website/blog is divided among Channel Register, which covers computer business and trade news, including business press releases. News and articles for computer hardware and consumer electronics is covered by Reg Hardware. Reg Research is an in-depth resource on technologies and how they relate to business. The whole blog is divided in sections such as Networks, Science, Security, Jobs, Business, Hardware etc.

As we can see, the nature of four selected blogs is rather different in terms of scope, ownership/operator and type of articles/posts provided. *Bemosa* and *Roger-Wilco* stand for highly specialized, narrow-topic weblogs in the area of airport security and air traffic management, respectively. Both are backed by private consulting companies, which can lead to skewed presentation of arguments favouring business interests of the two consultancies. Further, *Bemosa* blog is in fact a private blog of a single individual, Alan Kirschenbaum, who is accordingly also a single author of all posts. In contrast, *The Register* is rather a mass-impact, publisher-owned online magazine or newspaper with wide variety of topics concerning technology and related fields. It belongs among the leading global websites for IT specialists. The contributors are mainly specialized journalists. On the other hand, there is *HITB* – a blog operated by a non-profit company organizing security conferences in Malaysia and Netherlands, endorsed by various Malaysian governmental and non-governmental agencies. It concentrates mostly on IT security issues. The posts are usually very short and adopted from other online sources (blogs, IT news websites, online IT magazines, IT companies newsletters etc.), often in shortened version. The posts are tagged by topic and source and they usually contain number of readers figure, ranging from 1400 – 2000 per article.

3.3.2 The sample

To gather articles for analysis, all four blogs were searched for key words in English – 3D body scanners, Stuxnet and CCTV cameras. The results were then limited to articles published between 1st January 2010 and 31st April 2013 only. The search returned 345 articles in total, with most articles dealing with Stuxnet, which represented nearly 80% of the overall search return.

Table 2. Overall sample – Total hits

Blog	*The Register*	*HITB*	RW	*Bemosa*	**Total N**	**Total %**
Topic						
CCTV	36	11	0	1	**48**	**13.9**
Stuxnet	155	119	0	0	**274**	**79.4**
Body scanner	13	6	2	2	**23**	**6.7**
Total	**204**	**136**	**2**	**3**	**345**	**100**

After examining the articles more closely, we had to exclude a number of them, due to their irrelevance to the objectives of the study. Mostly, the reason here was that the article included the key word, but otherwise prevailingly referred to other topic. After selecting the relevant articles, the overall sample diminished to less than one half, with total number of articles being 150. Again, the majority of articles referred to Stuxnet (almost 70%), CCTV cameras were the topic of nearly 20% of articles and about 11% articles referred to 3D body scanners.

Table 3. Overall sample – Relevant articles

Blog	*The Register*	*HITB*	RW	*Bemosa*	**Total N**	**Total %**
Topic						
CCTV	23	5	0	1	**29**	**19.33**
Stuxnet	42	62	0	0	**104**	**69.33**
Body scanner	11	2	2	2	**17**	**11.33**
Total	**76**	**69**	**2**	**3**	**150**	**100**

As we can see in Table 4., the majority of relevant articles were posted in 2010 and 2011. However, there is no significant evidence of particular trends or peaks during time in monitoring particular issues in blogs, neither there is an evidence suggesting correlations with other phenomena. There are rather differences in bias of topic coverage among blogs. Although the issue of Stuxnet was generally very dominant, we can see that *The Register* was the most biased blog. The search returned 42 relevant articles for Stuxnet, but also 23 articles for CCTV cameras and 11 for 3D body scanners. *HITB* turned out to be very much focused on Stuxnet with the vast majority (62) of posts dedicated to this issue, whereas other two topics were covered by altogether 7 articles only. The reason here might be the orientation of blog prevailingly on IT issues. On the other hand, the other two blogs – *Roger-Wilco* and *Bemosa* returned very low number of articles. RW returned two articles for the issue of 3D body scanners and *Bemosa* returned one article for CCTV cameras and two articles dealing with 3D body scanners. This seems to be down to a highly specialized and narrow-topic nature of those blogs, which refer mostly to the issues of air traffic management and airport security. That’s also why no Stuxnet coverage was found, as IT issues are logically not the concern of these blogs.

Table 4. Relevant articles per topic and year

Blog	**Topic**	**Number of articles per year**				**Total**
		2010	2011	2012	2013	
The Register	CCTV	9	7	4	3	**23**
	Stuxnet	11	11	13	7	**42**
	Body scanner	7	3	0	1	**11**
HITB	CCTV	2	2	0	1	**5**
	Stuxnet	29	22	8	3	**62**
	Body scanner	0	1	1	0	**2**
RW	CCTV	0	0	0	0	**0**

	Stuxnet	0	0	0	0	**0**
	Body Scanner	2	0	0	0	**2**
Bemosa	CCTV	0	1	0	0	**1**
	Stuxnet	0	0	0	0	**0**
	Body scanner	0	1	0	1	**2**
Total		**60**	**48**	**26**	**16**	**150**

The quality of articles varied. The majority of articles found were rather short and informative reports, often taken from other online magazines, blogs and news agencies. Those generally contained no analysis at all or very limited one. Therefore, we had to be very careful with selection of articles for our sample. A method of purposeful sampling was used - the main criterion here was to select articles that would fit the objectives of our study to a maximum extent. In other words, from the articles relevant topic wise, we tried to choose rather longer ones, with maximum possible density of actors and arguments concerning our objectives. We also tried to keep the sample biased in terms of distribution of articles over time. However, this was not the primary aim for the reasons discussed earlier.

Table 5. Articles selected for analysis – final sample

Blog	***The Register***	***HITB***	**RW**	***Bemosa***	**Total**
Topic					
CCTV	6	1	0	1	**8**
Stuxnet	11	13	0	0	**24**
3D body scanner	3	2	2	2	**9**
Total	**20**	**16**	**2**	**3**	**41**

Altogether 41 articles were selected for the purpose of our analysis. The objective was to maintain the overall proportionality of topics and number of relevant articles returned by particular blogs. On the other hand, for the sake of more representative and biased final sample, some blogs and topics were over-represented and some under-represented compared to distribution of relevant articles overall sample. Table 6. shows the distribution of final sample of articles selected for analysis over time.

Table 6. Articles selected for analysis by year

Topic	**2010**	**2011**	**2012**	**2013**	**Total**
CCTV	3	3	0	2	**8**
Stuxnet	5	8	6	5	**24**
3D body scanner	3	3	1	2	**9**

Total	**11**	**14**	**7**	**9**	**41**

4 Analysis

The following section presents the findings of the qualitative textual analysis of the coverage and content of discussion on the topics of CCTV cameras, Stuxnet and 3D body scanners in selected expert online blogs between 1 January 2010 and 31 April 2013. We will focus on the actors involved in discussion, exact topics of their discussion, opinions and justification for actors' arguments. Further, we will concentrate on patterns of framing the topics in particular blogs and possible differences. The analysis is structured by topics.

4.1 CCTV cameras

Generally, the main issue discussed in articles we coded on CCTV cameras, was the controversy between security and privacy and personal data storage. The six articles (out of total of 8) from *The Register* blog, were relatively long and prevailingly contained quite a high level of analysis. The issue here was mainly the surveillance of citizen in the public areas and various counter-terrorist and anti-crime security projects of State police and local authorities in British environment. Special focus was put on ANPR system (Automated Number Plate Reader), used by the British police to monitor drivers. This system was mostly criticized, because of personal data gathering and its possible misuse. The same topic appeared in the *HITB* article, which was a very short report taken from other British online source, claiming that *"it was revealed today that the personal details of innocent motorists are being stored on a centralised database without their knowledge or permission."* (*HITB*, 05/04, 2010). On the other hand, a *Bemosa* blog article referred to security issues during the Olympic games in London and lessons to be learned from CCTV surveillance experience on airports, referring to a research generated on airport security claiming that about a third of security employees regularly bend and even break the rules and procedures when necessary. The article points out that such decisions are not made by individuals but as a group process and communications between security employees run along a parallel informal social network rather than the typical control command chain.

Table 7. Actors coded in relation to CCTV cameras

Actor	**Frequency**	**%**
Police	12	18,18
Advocacy Group/Civil society	12	18,18
State institutions	11	16,67
CCTV Cameras	6	9,09
Experts	6	9,09
City council	4	6,06
Municipality	3	4,55
Transport Company	3	4,55
Journalist	3	4,55
Politicians	2	3,03
Counterterrorism System	2	3,03
Private company	1	1,52
Activists	1	1,52
TOTALS:	**66**	**100**

As we can see in Table 7., the most frequent actors are the police (18%) and the advocacy groups of civil society (18%), followed by state institutions (16.7%). Police was mostly mentioned as an actor disposing with CCTV surveillance tools and storing personal data, being criticised by various groups of civil society. Following from this, the representatives of state institutions (such as the British Home Office) were generally defending or informing about security provisions and need of surveillance for the sake of public security. The articles also contained statements made by experts on surveillance, security and privacy (9%).

Table 8. Topics coded in relation to CCTV cameras

Topic	**Frequency**	**%**
Cameras CCTV	21	26,92
Surveillance	9	11,54
Personal data protection	9	11,54
Security related rules and regulations	7	8,97
Public domain monitoring	6	7,69
Purchase/Installation of CCTV cameras	5	6,41
Costs	5	6,41
Private domain monitoring	4	5,13
Surveillance Increase	4	5,13
Security General	3	3,85
Privacy	3	3,85
Crime Prevention	1	1,28
Personal freedom	1	1,28

TOTALS:	**78**	**100**

CCTV cameras themselves were coded as the most frequent theme of the statements (27%). Surveillance and personal data protection themes (both 11.5%) represent the main controversy within the whole topic area, which is logically closely connected to security related rules and regulations (9%) being the legal basis for surveillance from the side of state and the police. The public domain monitoring (7.7%) then constitutes a basic arena for such conduct. The blogs further typically brought information on CCTV cameras installations in new areas, leading to comments on costs of such systems (6.4%), e.g. *"Local authority spend on CCTV may be nearing the £500m mark according to The Cost of CCTV, a report by Big Brother Watch, published today."* (*The Register*, 30/11, 2010). Definitive argumentative strategies dominated among the coded statements, being rather informative and neutral. We coded 50 definitive statements, 2 evaluative and two advocative statements. The advocative statements were both negative, aimed against the use of CCTV cameras. As *The Register* writes, again quoting The Big Brother Watch (an advocacy group):

> *"Although proponents of CCTV claim that the figures will tend to be inflated by a larger upfront spend on installation, followed by lower year on year spend on maintenance, Big Brother Watch suggests that this assertion is questionable. Rather, it claims, the costs of maintenance, repair and upkeep represent a continuing significant drain on the public purse."* (*The Register*, 30/11, 2010).

The evaluative statements also came with a negative attitude. The representatives of civil society, The Big Brother Watch and No CCTV, were complaining about the costs, inefficiency and controversy in terms of lawfulness and accordance with democratic order. This example is concerned with ANPR systems, more specifically:

> *"The use of ANPR as a mass surveillance tool constitutes a major assault on our common law foundations and the rule of law," said Charles Farrier of No CCTV. "It is a system of automated checkpoints that ought to have no place in a democratic society."* (*The Register*, 13/6, 2011).

The only positive statements identified, were the ones of police representatives, defending the ANPR systems, claiming that the cameras are entirely lawful and highly efficient in targeting criminals and unsafe drivers.

Table 9. Argumentative strategies by direction of argument in relation to CCTV cameras.

Argumentative strategy	**Direction of argument**			**Total**
	positive	negative	neutral	
definitive	2	4	44	**50**
evaluative	0	2	0	**2**
advocative	0	2	0	**2**
Total	**2**	**8**	**44**	**54**

The justification for the actors' arguments could be identified in 23% of statements. As we could already see, the leading justifications were issues of efficiency, often meaning rather low efficiency of CCTV and issues of freedom/liberty, followed by costs. One another example for all, from already cited coded article, which quoted the Big Brother Watch report, including all the justifications at once, stressing costs and unefficiency:

> *"CCTV, the report claims, is "a costly placebo for many local authorities designed to appease neighbourhoods suffering from anti-social behaviour problems", doing little to solve real issues of crime. Councils 'spend shedloads on CCTV' and crime prevention, while ensuring that we are all now more watched than ever before."* (*The Register*, 30/11, 2010).

Table 10. Justifications in relation to CCTV

Justification	**Frequency**	**%**
Efficiency	5	21,74
Freedom/Liberty	5	21,74
Costs	3	13,04
Transparency	2	8,70
Right to Privacy	2	8,70
Security	1	4,35
National Security	1	4,35
Crime Prevention	1	4,35
Crime detection	1	4,35
Quality of service	1	4,35
Trust	1	4,35
TOTALS:	**23**	**100**

4.2 3D Body scanners

We coded altogether 9 articles dealing with the topic of 3D body scanners. Obviously, the topic of 3D body scanners relates by definition of its prevalent use to the main specialization of the two air traffic and airport security management blogs *Bemosa* and *Roger-Wilco*. It was also the only case, when RW blog entered our analysis, as the primary search returned two RW articles only, exclusively on the topic of 3D body scanners. Similarly, *Bemosa* blog covered the topic with two articles (out of three in total returned by primary search). The quality of articles varied massively. *The Register* brought articles with high informational value and reasonable arguments expressed by variety of actors, such as EU institutions, experts and advocacy groups. On the other hand, *HITB* posts were very short news reports, dealing with rather minor issues, such as reporting on a woman being caught and detected by body scanner with 44 iPhones. The second *HITB* article pointed out that it was possible to avoid the full body screening by officially paying to TSA (Transport Security Administration), which seems to be an interesting topic. Nevertheless, the article contained no analysis and arguments and was informative only. The *Bemosa* blog articles related directly to airport security and the role of human factor, passengers and security staff, and their attitude to security technology. Although the quality and expertise of these articles was beyond any doubt, there weren't many statements we could use for the objectives of our study. *Roger-Wilco* articles, on the other hand, contained very strong arguments, generally criticizing European institutions for inventing obstacles to prevent full body scanning introduction in the EU.

Table 11. Actors coded in relation to 3D body scanners

Actors	**Frequency**	**%**
Institutions	9	28,13
Advocacy Group/Civil society	4	12,50
Scanners	4	12,50
Experts	4	12,50
Transport Security Agency	3	9,38
Passengers	3	9,38
Journalist	2	6,25
State institutions	1	3,13
Politicians	1	3,13
Others	1	3,13
TOTALS:	**32**	**100**

The most frequent actors of the debate were institutions (28%), followed by civil society groups, scanners themselves and experts (12.5%). More specifically, the institutions were prevailingly EU institutions – the European Parliament, European Commission as a whole, EU

Transport Commissioner, the European Economic and Social Committee. These were mentioned mostly in relation to regulations concerning the introduction of 3D body scanners and debate about their efficiency versus health risks and privacy protection issues. The expert category included mostly health and radiation experts judging the levels of health risks. Advocacy groups of civil society could be divided in two categories – those concerned about privacy issues, such as EPIC (Electronic Privacy Information Centre) and those concerned with health risk issues, e.g. The American Pilots Association.

Table 12. Topics coded in relation to 3D body scanners

Topic	Frequency	%
Body Scanner	25	54,35
Security related rules and regulations	7	15,22
Privacy	6	13,04
Health issues	4	8,70
Freedom	2	4,35
Terrorism	2	4,35

Body scanner was coded as the most frequent theme of the statements (54%), followed by security related rules and regulations (15%), privacy (13%) and health issues (8.7%). The issues of freedom and terrorism appeared not to be very salient in the debate, which could be surprising in the latter case, as 3D body scanners are in fact meant to be a counter-terrorist measure. Apparently, the debate was more concerned about regulations of full body scanning in terms of privacy and health. This can be documented also with headline titles such as “*Warning cites radiation risk*” or “*Expensive, flaky, not fit for purpose*”. Rules and regulations coming from European Union institutions were significant topics of articles published on *Roger-Wilco* blog, being a subject of criticism due to alleged neglecting of security issues in exchange for human rights rhetorics.

Table 13. Argumentative strategies coded in relation to 3D body scanners

Argumentative strategy	**Direction of argument**			**Total**
	positive	negative	neutral	
definitive	1	7	19	27
evaluative	0	2	0	2
advocative	0	3	0	3
Total	**1**	**12**	**19**	**32**

Neutral definitive statements were identified as the most frequent type of statement. However, we coded also numerous statements with negative direction of argument. These statements were based on emphasis on health risks, e.g. *“The world's largest independent airline pilot association is warning its members to avoid security screening by full-body scanners out of concern the machines emit dangerous levels of radiation.”* (*The Register*, 9/11, 2010) or: *“In April, radiation experts from the University of California, San Francisco, warned President Obama's science assistant that the machines pose potentially serious health risks”*, sometimes pointed out the issue of efficiency and costs: *“The European Economic and Social Committee has delivered an opinion on scanner technology, which sets out concerns over the scanners' ability to improve security "which, coupled with the considerable cost of the scanners, remains the key issue".”* (*The Register*, 17/11, 2011). The civil society groups representatives further pointed out the human rights violation: *The group (Various Interest’s Group) slated the eroding of "fundamental rights" as a trade-off for public security, and said passengers should be able to opt out of searches without being hit with "additional burdens" such as delays or long queues. Efforts to rebrand body scanners as "security scanners" also got short shrift as a transparent attempt to make them "politically attractive".* (*The Register*, 17/11, 2011). A different example of negative direction statements would be *Roger-Wilco* articles evaluating negatively the performance of EU institutions blocking the introduction of body scanners: *“Shooting their mouth off about protecting human rights and so eventually blocking the introduction of full body scanning is nothing short of being misguided on the grandest scale possible. I would dearly like to know whether the MEPs really consider it preferable to be blown to kingdom come in the knowledge that no screener has seen their willy to arresting the one guy who is behind all the mischief”* (*Roger-Wilco*, 12/1 2010). Although being coded as negative statement, this obviously in fact strongly supports the idea of 3D body screening. Another supportive statement, coded as definitive but positive was expressed by EC Transport Commissioner Siim Kallas: *"Security scanners are not a panacea but they do offer a real possibility to reinforce passenger security,"* (*The Register*, 15/11, 2011).

Table 14. Justifications in relation to 3D body scanners

Justification	**Freguency**	**%**
Health	7	33,33
Privacy	4	19,05
Security	3	14,29
Efficiency	2	9,52

Freedom/Liberty	2	9,52
Legality	2	9,52
Costs	1	4,76
TOTALS:	**21**	**100,00**

As the coding of justification of the statements together with the quotations from the articles show, the prevalent justification related to body scanner were health issues, which was the case in one third of statements containing a justification. Privacy issues hold the second place in frequency among justifications (19%), followed by security (14.3%), efficiency, freedom and legality (9.5%). The issue of costs of body scanning was not particularly significant in the debate.

4.3 Stuxnet

The topic of Stuxnet worm was the most salient one as far as expert blog analysis is concerned. Article search returned almost 70% of overall number of relevant articles, which is really a very significant dominance of one topic. However, two of blogs analyzed did not return any articles related to Stuxnet. Not surprisingly, these were the highly specialized "airport" blogs – *Roger-Wilco* and *Bemosa*, as this topic does not fit in their area of expertise. From the two blogs left, *HITB* returned the most of the articles. Altogether, we coded 13 *HITB* articles and 11 articles from *The Register*. Although we might say that the quality of *HITB* articles related to this topic was generally higher, compared to previous topics in terms of expertise and informational value, the articles were still very short, adopted from other online sources and not offering in-depth analysis and interaction of actors. Nevertheless, it is evident, that the topic of cyber security and hacking significantly attracted the attention of this particular blog community, since this area appears to be its main field of interest. *HITB* articles were generally informing about the Stuxnet worm attack on Iran, were bringing news on Iran official's reactions to the attack and speculations about origin and motivations of the attack as well as about states and organizations involved. The second theme might be defined as the future of cyber security in post-Stuxnet world, that means the possible future threats and their solutions.

The latter theme also fits with the main focus of the most of *The Register* articles. These were again of a high quality, often containing an in-depth analysis and bringing in various actors making strong statements and bringing arguments. That is also a reason for a bit of an over-representation of *The Register* articles in our final sample. The articles generally mostly referred to issues of cyber security challenges after Stuxnet attacks, possible danger of cyber war and legal implications of cyber terrorism, including implications to international law.

Table 15. Actors and their origin coded in relation to Stuxnet

Actor	**Frequency**	**%**	**Actor's origin**						
			Iran	United Kingdom	Israel	USA	China	Russia	supranational
Experts	34	34	1	1		2			
State institutions	22	22	6		3	13	1	1	1
Stuxnet	10	10							
media	8	8	1		1	5			1
State(s)	6	6	4		2				
Journalist	4	4							
Israel secret service	3	3			1				
Private company	3	3							
Virus/Malware/Worm	3	3							
President	2	2				2			
Non-state institutions	2	2							
Institutions	1	1							
National Security Agency	1	1				1			
other groups	1	1							
TOTALS:	**100**	**100**	**12**	**1**	**6**	**20**	**1**	**1**	**2**

Experts were coded as the most frequent actors (34%), followed by state institutions (22%) and Stuxnet itself (10%). The experts' origin was often not explicitly mentioned, mostly being private company computer security experts, computer scientists, or legal experts. On the other hand, the origin of the second most frequent actor, state institutions, was often explicitly expressed in the statements. We identified 15 cases of USA state institutions, being the actor, including the President of USA, cited "senior USA officials" and Chiefs of Government Departments. We also identified 6 cases of Iranian state institution actors, including the Iranian president, Chief for Atomic Energy and other "Iranian officials". The other state institution actors were Israel (3), China, Russia (both 1) and one supranational actor – OSN.

Table 16. Topics coded in relation to Stuxnet

Topic	**Frequency**	**%**
Cyber war	24	14,20

Stuxnet	23	13,61
Attack on Iran	15	8,88
USA	12	7,10
Israel	12	7,10
Development of Stuxnet by a state	11	6,51
Deployment/attack using Stuxnet	11	6,51
Development of Stuxnet	10	5,92
Flame	10	5,92
Counter-Attack	7	4,14
Legality	6	3,55
Attack	6	3,55
Security General	5	2,96
Attack on a company	5	2,96
Iranian uranium enrichment programme	4	2,37
Olympic games	4	2,37
State accused of attack	2	1,18
Attack on other state	2	1,18
TOTALS:	**169**	**100**

Cyber war was coded as the most frequent theme (14.2%), almost together with Stuxnet itself (13.6%), followed by themes of attack on Iran, USA, Israel, development of Stuxnet by a state and deployment/attack using Stuxnet. This very well portraits, what was already said earlier, when generally characterizing the articles. One part of articles was rather informative, relating to the Stuxnet attack itself and the reactions of international community and Iran as the target of the attack and searching for the attacks origin. E.g.: "*Iran's atomic energy chief said that a delay in the launch of the nation's first nuclear power plant was not caused by a powerful computer virus that has crippled data management systems across the world -- but his explanation may not have reassured Persian Gulf residents.*" (*HITB*, 4/10, 2010) or:

> "*Russia has for the first time laid the blame for the Stuxnet worm at the door of the US and Israel, describing it as "the only proven case of actual cyber-warfare."In translated comments reported by the AFP agency, foreign ministry security department chief Ilya Rogachyov was blunt about the origins of a piece of malware that has mystified experts since first appearing in June 2010.*" (*HITB*, 26/9, 2012)

The second part of the articles related to the issues of international cyber security, possibility of future cyber war and changing nature of international warfare. Also, we could identify accents on the need of new legal framework, establishing what is a cyber-attack and if (or how) it is legal for a country to defend itself. E.g.:

> *"Instead of a standalone war in cyberspace, it is far more likely that cyber-conflicts will take place alongside conventional attacks by nation states and propaganda offensives. Cyber-spying is a real enough threat but it isn't helpful to conflate this threat with cyberwar – cyberespionage is not a "few keystrokes away from cyberwar", the authors argue."* (*The Register*, 17/1, 2011*).*

Another article quotes a NATO backed legal experts manual establishing the rules of cyber-war:

> *"Cyber-attacks primarily designed to spread terror are classified as unlawful (rule 36) but cyber-propaganda is allowed. Attacks against dual-use military and civilian systems, including computer networks, are permitted (rule 39)"* (*The Register*, 20/3, 2013).

Table 17. Argumentative strategies coded in relation to Stuxnet

Argumentative strategy	**Direction of argument**			**Total**
	positive	negative	neutral	
definitive	4	4	78	**86**
evaluative	0	0	0	**0**
advocative	0	1	0	**1**
Total	**4**	**5**	**78**	**87**

The vast majority of coded statements were definitive and neutral, since the experts as main actors were prevailingly tending to be objective and neutral. Further, the state institutions as actors were not trying to be objective, but their statements were representing their definitive standpoints. Definitive statements with negative direction were mostly expert statements not favoring the discussed possibility of cyber war:

> *"It is unlikely that there will ever be a true cyberwar. The reasons are: many critical computer systems are protected against known exploits and malware so that designers of new cyberweapons have to identify new weaknesses and exploits; the effects of cyberattacks are difficult to predict – on the one hand they may be less powerful than hoped but may also have more extensive outcomes arising from the interconnectedness of systems, resulting in*

> *unwanted damage to perpetrators and their allies. More importantly, there is no strategic reason why any aggressor would limit themselves to only one class of weaponry."* (*The Register*, 17/1, 2011).

Table 18. Justifications in relation to Stuxnet

Justification	**Frequency**	**%**
Efficiency	7	29,17
Deffense	5	20,83
Premptive strike	4	16,67
Security	3	12,50
Costs	2	8,33
Legality	2	8,33
Expert opinion	1	4,17
TOTALS:	**24**	**100**

Although we coded the largest number of statements compared to other two topics (100 statements), we were able to identify justifications in only 24 statements. Efficiency was the most frequent one (29%), followed by defense (20.8%) and preemptive strike (16.7%). Efficiency justification was mostly used when referring to Stuxnet worm and its efficient harmful power. Defense and preemptive strike were most frequently used by legal experts when justifying the right to carry out a cyber-attack for the purposes of defense:

> *"Schmitt said the legal experts who drew up the manual agreed that Stuxnet was an act of force but were divided on whether the malware constituted an armed attack. And even if it was an armed attack it might still be justified as self defense in the form of striking back at the aggressor in the face of imminent attack" (The Register, 9/10 2010).*

5 Summary: Actors and Argumentative Strategies in Expert Blog Articles referring to 3D Body Scanners, CCTV cameras and Stuxnet

There were major differences concerning the level of particular topics coverage among the blogs analyzed. This also applies to bias of topics as well as to overall numbers of relevant articles found within particular blogs. However, no evidence or tendency could be found in respect of linkage of particular events and the debate content across time in the timespan selected, as far as our analysis is concerned. Generally, the issue of Stuxnet was very dominant, with almost 70% of articles referring to the topic. CCTV was the topic of nearly 20% of blog posts and about 11% of them dealt with 3D body scanners. *The Register* turned to be relatively the most biased blog concerning the distribution of topics, although Stuxnet still dominated. The other three analyzed blogs showed rather a narrow-topic nature, concentrated prevailingly on issues of IT security as *Hack in the Box* (*HITB*) or exclusively on issues of air traffic management and airport security – *Roger-Wilco* and *Bemosa* blogs. The latter two blogs also returned a very low number of articles. Consequently, this brings certain limitations for comparative perspective among topics, as some blogs and topics were intentionally over-represented and some under-represented compared to distribution of relevant articles in our overall sample.

Table 19. Overall sample – Relevant articles

Blog	*The Register*	*HITB*	RW	*Bemosa*	**Total N**	**Total %**
Topic						
CCTV	23	5	0	1	**29**	**19.33**
Stuxnet	42	62	0	0	**104**	**69.33**
Body scanner	11	2	2	2	**17**	**11.33**
Total	**76**	**69**	**2**	**3**	**150**	**100**

Starting with the two less salient topics in expert blog discourse content analysis – 3D body scanners and CCTV cameras, we can observe a relative closeness in terms of actors making statements. In both cases, state institutions and civil society advocacy groups were entering the debate the most. In the case of CCTV cameras, also police would be included, being regarded as a law-enforcing state institution. As for the 3D body scanners, institutions were by far the most frequent actor, prevailingly meaning EU institutions – the European Parliament, European Commission, European committees etc. The CCTV cameras debate, on the other hand, involved mostly national institutions, prevailingly British. These similarities seem to arise from the analogous core of the debate within these two topics, lying in introduction or disposal of certain controversial security measures by national/European institutions towards citizen. Advocacy groups/Civil society actors were then making statements responding to such behaviour. Concerning 3D body scanners, also numerous experts were entering the debate, mostly being health and security professionals. The main points of the related discourse were the regulations concerning the introduction of 3D body scanners and their efficiency versus health risks and privacy protection issues. Health was also the top ranking statement justification, used mainly by experts and workers advocacy groups, judging the risks of 3D body scanning. Justifications by privacy followed, mostly from the side of civil society groups concerned about privacy issues, such as EPIC (Electronic Privacy Information Centre).

Quite surprisingly, the more general issues of counter-terrorism protection and arising limitations to personal freedom, appeared not to be very salient in the debate, although 3D body scanners are in fact meant to be a counter-terrorist measure. However, in the expert blog discussion related to CCTV cameras, the limitations to personal freedom were a major controversy, represented by surveillance of citizen in public areas and personal data protection themes. Security related rules and regulations constituting a legal basis for surveillance from the side of state and policy, was then mostly criticized by representatives of civil society. The leading justifications of such statements were issues of low efficiency, freedom/liberty and costs. The representatives of state institutions and police, on the other hand, were informing on or defending the CCTV security measures, arguing by its high efficiency and positive effects on public security.

As far as the expert blog analysis is concerned, the topic of Stuxnet was by far the most salient one and was also significantly different from the two other topics. Apparently, the topic of cybersecurity and hacking attracted the attention of this particular blog community, since this area appears to be its main field of interest. Given the global nature of the Stuxnet worm, the variety of actors identified was much higher, encompassing international Experts, State institutions and Media as the most frequent ones. The exact origin of experts was rather unspecified, while especially state institutions were often nation-identified, with USA state institutions being the most frequent, followed by Iranian and Israeli institutions. Generally, analyzed articles were either informative about the Stuxnet attack on Iran, or focusing on the issues of cyber security challenges after Stuxnet attacks. That implies the three most frequent topics – Cyberwar, Stuxnet itself and Attack on Iran.

Concerning argumentative strategies used, the majority of coded statements was definitive and neutral, so as was the case throughout all of the three studied key topics. In case of Stuxnet, experts as the main actors were prevailingly tending to be objective and neutral, whilst state institutions as the second most important actor were presenting their definitive statements, though not trying to be objective. The statement justifications employed Efficiency in the first place, followed by Defense and Preemtive strike. Efficiency was mostly referring to Stuxnet as an efficient harmful power, while Defense and Preemptive strike were frequently used by legal experts when justifying the right to carry out a cyber-attack for the purpose of defense.

Table 20. Argumentative strategies by direction of argument - Total

Argumentative strategy	**Direction of argument**			**Total**
	positive	negative	neutral	
definitive	7	15	141	**163**
evaluative	0	4	0	**4**
advocative	0	6	0	**6**
Total	**7**	**25**	**141**	**173**

In sum, justifications to statements could be found in approximately 25% of analyzed statements, with exception of 3D body scannners, where the rate reached about 68%. As already mentioned, the vast majority of coded statements were neutral and definitive. There were only 4 evaluative and 6 advocative statements out of total of 173. However, some topics showed a higher rate of negative direction arguments, such as 3D body scanners, where negative direction of argument was observed in approx. one third of statements (both definitive, evaluative and advocative). Those were raised mostly by civil society representatives criticizing the introduction of scanning. As for positive directions of arguments, these were rather rare (only 7 out of 173). Two of them related to CCTV cameras, one to 3D body scanners and four to Stuxnet.

6 Conclusion

This study provided results of qualitative textual analysis of the coverage and content of discussion on the topics of CCTV cameras, Stuxnet and 3D body scanners in selected expert online blogs between 1 January 2010 and 31 April 2013. We could see that the domain of online expert blogs is a specific area that might differ a lot from the scope and nature of traditional printed media. This is of course given by their global online outreach, increased immediacy, interactivity and interdependence with other sources. At the same time, the blog writing needs not to be following the standards and practices of traditional media, such as balance in viewpoints or facts-based reporting. The significant differences among blogs in terms of scope, ownership/operator and type of articles/posts provided, brings serious limitations to comparability and bias of such analysis. Further, we have to bear in mind that appart from the differences in aim-readers of particular blogs (e.g. IT community, air-traffic professionals or wider general public), also various pertinent bussiness interests may come in play. Two of the blogs analyzed (*Bemosa and Roger-Wilco)* are backed by private consulting companies, which can lead to skewed presentation of arguments favouring business interests of the two consultancies. On the other hand, there is a mass-impact, publisher-owned online magazine or newspaper, belonging among the leading global websites for IT specialists and *HITB* – a blog operated by a non-profit company organizing security conferences in Malaysia and Netherlands, endorsed by various Malaysian governmental and non-governmental agencies. It is obvious that business interests concerning the advertising, funding and readership support can be nothing but significantly distinct, which may have impact on the composition and character of published aticles. Nevertheless, we believe that conducted analysis may still serve as a valuable insight in coverage and manner of coverage of our three security topics among a highly specialized community. The analysis showed, that despite the fact that the selected blogs should contain expert opinions, the quality of articles varies a lot. The most informative but also least analytical blog was the *HITB* blog. It is merely an announcement blog as it concentrates short and media agency news from the security industry, with focus on cyber security, but does provide only very limited analytical contributions. The *Bemosa* and *Roger-Wilco* blogs are also focusing on very narrow topics, but they provided high quality articles. Yet due to their high specialization, they offered only a limited scope of useful information for the objectives of our study. Only *The Register* blog proved to be a very sophisticated source of information and provided in-depth discussion among the readers community.

To conclude, the results of our analysis framed by the selected time period and the four expert blogs chosen, have shown that in terms of saliency, the topic of Stuxnet worm was significantly dominant within the expert security blogs (about 70% of the relevant articles found). Suggested reason would be that the focus of the prevailing and most fertile part of the blogosphere analysed, is based in IT issues (*HITB*, *The Register* – originally an IT technology news site, though currently more broad-oriented). Therefore, the matters related to cyber security and hacking seems to be the closest point of interest. CCTV cameras and 3D body scanners followed with 20% and 11%, respectively. Assessing the nature of discussion generally, we could say that although the blogs are considered to be expert oriented, the debate here was not very expert or technical. An extensive portion of articles was rather short and informative. Articles with more in-depth analysis then could be described as rather opinion oriented, without getting too much into specific technicalities. An exception would be a legal analysis of possible implications of cyber-security discussion after Stuxnet attacks for international law (“Stick nuke plants and hospitals on no-go list too - war manual“, *The Register*, 20/03 2013). It was also the Stuxnet topic, where the questions of security were raised the most, referring to cyber security challenges in post-Stuxnet world and possible dangers of cyber war, including legal implications. Concerning other two topics, CCTV cameras and 3D body scanners, the issues of privacy protection needs against security measures clearly dominated. A voice was given more to the experts and other actors criticizing the security measures arguing with privacy and human rights issues, health risks, costs and inefficiency. On the other hand, we could find also support for security measures, particularly 3D body scanners, especially in air-traffic management oriented blogs.

As we could see, though the “blogosphere” is not straightforward to handle, it can offer a valuable contribution to media content analysis, as the area of new social media is definitely still growing in importance and dynamics.

7 References

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

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

De Zuniga,H., E.Puig-I-Abriland, H.Rojas. 2009. “Weblogs,TraditionalSourcesOnlineandPolitical Participation: An Assessment of How the Internet Is Changing the Political Environment“, *New Media & Society* 11(4), pp. 553-74.

Drezner, D.W. and H. Farrell (2004) “The Power and Politics of Blogs“, paper presented at the American Political Science Association 2004, Chicago, IL, September

Guasti, Petra. 2013. “Prague Graduate School in Comparative Qualitative Analysis 2013“ *SECONOMICS Newsletter*, 2013/1, Prague: Academy of Sciences of the Czech Republic.

Mazur, Allan. 2006. “Risk Perception and News Coverage across Nations“, *Risk Management*, Vol. 8, No. 3, pp. 149-174

Meraz, S. 2007. “Analyzing Political Conversation on the Howard Dean Candidate Blog’, in M. Tremayne (ed.) Blogging, Citizenship, and the Future of Mediapp.59–82. New York: Routledge

Vrablikova, Katerina. 2012. “Risk Perception research: Literature and Data review.” *Prague SECONOMICS Discussion Papers* 2012/1. Prague: Academy of Sciences of the Czech Republic.

Wiegman, O., Gutteling, J., Boer, H. and Houwen, R. 1989. „Newspaper Coverage of Hazards and the Reactions of Readers“, *Journalism Quarterly*, 66, pp. 164-193.

Williams, J. and F. Massacci. 2013. “Editorial“ , *SECONOMICS Newsletter*, 2013/1, Prague: Academy of Sciences of the Czech Republic.

“Journalists and Social Media“ – Eurobarometer Aggregate Report, January 2012

8 Appendix

List of analyzed articles by topic:

Articles downloaded from following websites in search period between 1st January 2010 and 31st April 2013:

Bemosa - http://bemosa.blogspot.com
Roger-Wilco - http://www.roger-wilco.net
Hack in the Box – HITB - http://www.HITB.org
The Register - http://www.theregister.co.uk

CCTV cameras

Outrage over another secret police database, *HITB*, 04/05 2010 (news.hitb.org/content/outrage-over-another-secret-police-database)

On CCTV, privacy, data protection..., *The Register*, 05/10 2010 (www.theregister.co.uk/2010/10/05/project_champion_report/)

Report shows costly cost of local snoopage, *The Register*, 30/11 2010 (www.theregister.co.uk/2010/11/30/big_brother_watch_cctv/)

Code of practice in surveillance leaves little to protect privacy, *The Register*, 16/02 2011 (www.theregister.co.uk/2011/02/16/freedoms_bill_promotes_surveillance/)

Ought to have no place in a democratic society, *The Register*, 13/06 2011 (www.theregister.co.uk/2011/06/13/anpr_plan_panned/)

Watching security at the London olympics through an airport prism, *Bemosa*, 10/08 2011 (bemosa.blogspot.cz/2011/08/london-olympics-security.html)

Miscreants can copy, delete streams and even control the device, *The Register*, 29/01 2013 (www.theregister.co.uk/2013/01/29/cctv_vuln/)

'Surveillance by consent' but operators WON'T BE sanctioned for cockups, *The Register*. 08/02 2013 (www.theregister.co.uk/2013/02/08/uk_cctv_draft_code_of_practice/)

3D Body scanners

Is being blown up part of my human rights?, *Roger-Wilco*, 12/01 2010 (www.roger-wilco.net/tag/security/page/2/)

European Parliament – The terrorists’ best friend?, *Roger-Wilco*, 13/02 2010 (www.roger-wilco.net/european-parliament-—-the-terrorists’-best-friend/#more-5906)

Warning cites radiation risk, *The Register*, 09/11 2010 (www.theregister.co.uk/2010/11/09/pilots_oppose_backscatter_scanners/)

Woman Caught at Airport with 44 IPhones Hidden in Her Stockings, *HITB*, 30/01 2011 (news.hitb.org/content/woman-caught-airport-44-iphones-hidden-her-stockings)

Nudie-watching staff kept away from passengers, *The Register*, 15/11 2011 (www.theregister.co.uk/2011/11/15/eu_airport_body_scanner_rules/)

Expensive, flaky, not fit for purpose ..., *The Register*, 17/11 2011 (www.theregister.co.uk/2011/02/17/scanner_opinion/)

Pay the TSA $100 and they'll let you bypass airport security screening, *HITB*, 16/03 2012 (news.hitb.org/content/pay-tsa-100-and-theyll-let-you-bypass-airport-security-screening)

Why passengers and security personal don’t trust technology?, *Bemosa*, 13/05 2013 (bemosa.blogspot.cz/2011/12/passengers-airport-security-personal.html)

Body Scanner: Who says looks don’t count?, *Bemosa*, 16/05 2013 (bemosa.blogspot.cz/2013/01/body-scanner-who-says-looks-dont-count.html)

Stuxnet

Iran says Stuxnet not to blame for delay in power plant launch, *HITB*, 04/10 2010 (news.hitb.org/content/iran-says-stuxnet-not-blame-delay-power-plant-launch)

Stuxnet worm attacks no longer just Hollywood hype, *HITB*, 27/10 2010 (news.hitb.org/content/stuxnet-worm-attacks-no-longer-just-hollywood-hype)

International intrigue puts security on global stage, *HITB*, 14/12 2010 (news.hitb.org/content/international-intrigue-puts-security-global-stage)

EU agency warning, *The Register*, 09/10 2010 (www.theregister.co.uk/2010/10/09/stuxnet_enisa_response/)

Stuxnet’s Finnish-Chinese Connection, 15/12 2010 (news.hitb.org/content/stuxnet’s-finnish-chinese-connection)

Pure cyberwar? Not gonna happen, *HITB*, 17/01 2011 (news.hitb.org/content/pure-cyberwar-not-gonna-happen)

Night Dragon Stalks Oil and Gas, *HITB*, 13/02 2011 (news.hitb.org/content/night-dragon-stalks-oil-and-gas)

DHS chief: What we learned from Stuxnet, *HITB*, 26/04 2011 (news.hitb.org/content/dhs-chief-what-we-learned-stuxnet)

Cyberwar, Stuxnet and people in glass houses, 07/06 2011 (news.hitb.org/content/cyberwar-stuxnet-and-people-glass-houses)

The ill-informed leading the ill-informed..., *The Register*, 17/01 2011 (www.theregister.co.uk/2011/01/17/cyberwar_hype_oecd_study/)

Hague convention for state-backed hacking?, *The Register*, 04/02 2011 (www.theregister.co.uk/2011/02/04/cyberwar_rules_of_engagement/)

Post Stuxnet – expect government hacking, *HITB*, 08/04 2011
(news.hitb.org/content/post-stuxnet-—-expect-government-hacking)

SCADA maker 'provided the enemies' with help, *The Register* 18/04 2011
(www.theregister.co.uk/2011/04/18/iran_blames_siemens_for_stuxnet/)

AusCERT: What is cyberwar anyway?, *The Register*, 16/05 2012
(www.theregister.co.uk/2012/05/16/stuxnet_was_not_cyberwar/)

Well, sure ... so why are you telling us, Mr President?, *The Register*, 01/06 2012
(www.theregister.co.uk/2012/06/01/stuxnet_joint_us_israeli_op/)

Israel blamed for cyberweapons' escape into the wild, *The Register*, 20/06 2012
(www.theregister.co.uk/2012/06/20/us_israel_flame/)

Stuxnet: 'Moral crime' or proportionate response?, *HITB*, 27/07 2012
(news.hitb.org/content/stuxnet-moral-crime-or-proportionate-response)

Russia blames US and Israel for Stuxnet worm, *HITB*, 26/09 2012
(news.hitb.org/content/russia-blames-us-and-israel-stuxnet-worm)

'And Iran to prosecute American programmers for Stuxnet?', *The Register*, 20/12 2012
(www.theregister.co.uk/2012/12/20/prosecute_foreign_hackers_plan/)

Unseen, all-out cyber war on the US has begun, *HITB*, 30/01 2013
(news.hitb.org/content/unseen-all-out-cyber-war-us-has-begun)

FBI intent on sniffing out those who leaked possible US Stuxnet role, *HITB*, 30/01 2013
(news.hitb.org/content/fbi-intent-sniffing-out-those-who-leaked-possible-us-stuxnet-role)

New training program to create youth hacking force, *The Register*, 02/02 2013
(www.theregister.co.uk/2013/01/02/israel_cyberwarfare_training_for_teens/)

Stick nuke plants and hospitals on no-go list too - war manual, *The Register*, 20/03 2013
(www.theregister.co.uk/2013/03/20/cyberwar_rules/)

Would you rather be shot, blown up, stabbed - or hacked?, *The Register*, 27/03 2013
(www.theregister.co.uk/2013/03/27/stuxnet_cyberwar_rules/)