Prague SECONOMICS Discussion Papers
2014/1

Report on Expert Blogs Analysis

Contribution to the SECONOMICS project and
Prague Graduate School in Comparative Qualitative Analysis 2013

Tomáš Lacina

Institute of Sociology
Academy of Sciences of the Czech Republic
Prague, January 2014

Editorial Board: Zdenka Mansfeldová, Petra Guasti, Jessie Hronešová
Copy-editing: Robin Cassling
Published by: Institute of Sociology, AS CR
Jilská 1, 110 00 Prague 1
Prague 2014

Contact: Press and Publications Department
Institute of Sociology, AS CR
Jilská 1, 110 00 Prague 1
tel.: 210 310 217
e-mail: prodej@soc.cas.cz

This publication has been completed with funding from project SECONOMICS: Socio economics meets security, an Integrated Project supported by the European Commission's Seventh Framework Programme for Research, theme SEC-2011.6.4-1 SEC-2011.7.5-2 ICT.

ISBN 978-80-7330-249-8

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

In this discussion paper series, the Prague *SECONIMICS* team intends to allow the broader academic community taking part in an on-going discussion about risks and threats as well as trade-offs between them and security. This research focus stems from the fact that until now, social scientists have primarily studied threats and risks through the perspective of social psychology by conducting the so-called "risk assessment" analyses, especially looking at the concept of "risk perception". This research thus aims to probe these concepts in order to broaden our understanding of the multivariate study of risks and threats in social sciences by adding some context-dependent and temporal aspects.

Table of Contents

1 Introduction

Every day the daily news coming from various parts of world can only confirm our conviction that security issues are among the most salient concerns of contemporary societies. Moreover, in the globalised system, various conflicts, risks, and other security issues naturally become global, transcending 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 are faced with new types of risk, which are mainly a product of human activity, such as nuclear radiation, global warming, financial crises, and terrorism (Beck 1992 and Beck 2002). Beck (1992) claims that these new risks have become the central dynamics that characterise contemporary societies and have led to the transformation of society as a whole and the social order (Vrablikova 2012). Within this context, it seems reasonable to raise questions about the perception of risk by individual citizens and the differences in risk perception among various groups. This implies further questions concerning the impacts of various risk perceptions on human behaviour, political decision-making, and the economy. This range of issues constitutes an important part of the objectives of the SECONOMICS project, which is a broad cross-disciplinary 7FP project aimed at providing a socio-economic rationale for 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 trace out the main issues in security management. The scientific research behind the project is founded on models of game theory, systems modelling, adversarial risk analysis, and social policy applied in a unified framework. This framework should provide policy-makers with insight that they can use to design an effective security policy and security investments and to understand the public acceptance of security and the incentive structure of individuals and organisations with respect to security (Williams and Massacci 2013).

The results of a quantitative secondary data analysis of existing studies on risk and threats using cross-national surveys offer an important general overview of citizens' perceptions and attitudes towards risk and security (Guasti 2013). However, the use of secondary sources proved to be of limited relevance for the SECONOMICS case studies. Consequently, it was necessary to supplement these data, which was done by putting together a collection of qualitative data drawn from print media. The media analysis conducted in the scope of this project offered a good basis for comparative analysis of the communication channels and communication patterns that exist between policy-

makers, stakeholders, and citizens in the area of security (Guasti 2013). Moreover, media have an important 'agenda-setting' effect, bringing certain issues to the forefront in the minds of people, including policy-makers. This ability of mass media to direct public attention and governmental action towards specific policy concerns has been documented in many cases - for example, in the area of risks to health and the environment (Mazur 2006, Wiegman et al. 1989). This force function of media also constitutes an important factor of the relevance of media analysis in the field of security issues. The news analysis was supplemented by an analysis of four selected English-language expert security blogs to obtain a deeper insight into communication patterns among those inside the security expert community. Blogs appear to be of increasing importance with the rapid growth of new media and online journalism. There is more and more evidence showing that the internet has a reinforcing effect on information-seeking and sociability. Certain forms of internet use contribute to civic engagement and trust, increase volunteerism, enhance personal interactions, and increase news consumption (Gil de Zuniga et al. 2009). However, it appears it is not just the migration of traditional news sources online that is the cause of this, but that the emergence of an interactive opinion space of personal journals or weblogs (blogs) is also a factor.

The aim of this study is to present the findings of an analysis of expert security blogs that was carried out between 1 January 2010 and 30 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?

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

2 Background

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 more. The common attribute of social media is that they turn communication and news consumption into an interactive dialogue. Research conducted among European journalists (Eurobarometer 2012) has shown that journalists primarily use social media in the broader process of compiling stories, promoting them, and getting feedback from the public. Research also shows that social media are regarded as extremely useful and easy to use. The only concern that has been raised regards the credibility of the information (Journalists and Social Media – Eurobarometer Aggregate Report, January 2012).

There is no generally agreed definition of blogs. They can be defined as online interactive journals that facilitate information exchange between users called 'bloggers' and that have a particular style of writing. Topics are usually arranged in reverse chronological order and information is periodically updated by the blog's administrator (Gil de Zuniga et al. 2009). Blogs can function as personal diaries, technical discussions, sports commentary, celebrity gossip forums, political discussion sites, or all of the above (Drezner and Farrell 2004). Blogs distinctively incorporate links to other blogs, webpages, forums etc., making them interconnected and interdependent, and some of them become central (Drezner and Farrell 2004). They are interactive, non-synchronous webpages, whose host uploads postings centred on a certain topic. The writing need not follow the standards and practices of traditional media, such as maintaining balance of viewpoints, fact-based reporting, and so forth (Gil de Zuniga et al. 2009).

The blogosphere has grown at an astronomical rate, from numbering in the thousands in the year 2000, to a range of 2.1–4.1 million in 2003, and finally to 133 million blogs 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). As the importance of blogs has risen they 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 an environment of user control, content richness, increased

immediacy, and interactivity, and they provide audiences with control over multiple choices (Meraz 2007). The participatory and autonomous nature of blogs has made them a central part of the new media landscape (Kraushaar 2009).

The amount of attention traditional media devote to blogs has also increased dramatically. As the blogosphere has grown, a variety of institutions have adopted blog form. Many journals, newspapers, and the websites of TV news 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), a sign of the links between the political and expert parts of the blogosphere and the media sphere. This makes blogs even more relevant and influential within the general media context. A reason for this may be that expert blogs offer specialised and detailed knowledge on wide range of issues, thus greatly reducing the search costs for traditional journalists. Furthermore, bloggers have first-mover advantages in formulating opinions. The speed of blogger interaction can have an agenda-setting effect on the mainstream media – for example, if a critical number of elite blogs raise a particular story, this may 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 the specific topics of our study.

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

As regards air-traffic terrorism, there were a number of attempted airliner bombings in 2000-2010. One was the case of Northwest Airlines Flight 253, an international passenger flight from Amsterdam, the Netherlands, to Detroit, United States that was the target of

a failed al-Qaeda bombing attempt on 25 December 2009, when a passenger tried to set off plastic explosives sewn to his underwear. Other examples are the Russian aircraft bombings of August 2004, the terrorist attacks on two domestic Russian passenger aircraft flying from Moscow's Domodevo Airport, and the 2006 terrorist plot to detonate liquid explosives carried on board at least 10 aircraft flying 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 sparked discussion and the proposal to introduce **full-body scanners**, which are capable of detecting non-metal objects carried by passengers. In 2007, full-body scanners started to replace metal detectors at airports and train stations in many countries. Some passengers and public interest advocates have objected to the idea of pictures of their naked bodies being displayed to screening agents or recorded by the government. Some critics have called this form of imaging virtual strip-searches without probable cause, and some have claimed they are illegal and violate basic human rights. In 2007, a US federal appeals court ruled in a lawsuit brought by the Electronic Privacy Information Center that even scanners that produce a nude image of the body are within the bounds of what can be considered a reasonable and constitutional security check. In the United States, federal law requires that from June 2013 all full-body scanners must use software that replaces the nude image with animated image of the body.

With respect to the subject of **CCTV cameras** and public surveillance, a strong debate was sparked by measures recently adopted in the United Kingdom. Following pilot tests (e.g. Project Laser or Project Spectrum), CCTV cameras with automatic number plate recognition have been installed on most motorways, main roads, town centres, ports and petrol station forecourts since March 2006. Traffic cameras in towns and cities are being converted to read number plates automatically as part of the new national surveillance network. Police have immediate access to all camera data. Effectively, the police (and the security services) can track any car around the country almost in real time. Although CCTV generally has public and political support in the United Kingdom, there are privacy concerns in the face of the integration of the different systems and databases - such as linking car number plate recognition cameras to personal data. Moreover, in some areas the installation of an ANPR system generated so much controversy that it was later suspended. This was the case of Project Champion, a project to install a network of ANPR cameras to monitor vehicles entering and leaving

two neighbourhoods in Birmingham in which there are large Muslim communities. Its implementation was frozen in June 2010 amid allegations that the police deliberately misled councillors about its purpose, allegations that arose once it was revealed that the project was being funded as an anti-terrorism initiative, not for 'reassurance and crime prevention'.

3 Methodology

3.1 Research design

In this paper, qualitative textual analysis of blog posts is used to create a basis for further comparative qualitative analysis at a later stage in the research. The analysis is centred on three security issues that were studied in the SECONOMICS case studies: 3D body scanners, Stuxnet, and CCTV cameras. The main research questions of this study are: How salient are the selected topics among security bloggers? How do expert blogs frame the implications of security and security technologies in the context of our three SECONOMICS topics? What is the perception of security risks among the security expert blog community? Do questions of security dominate as opposed to issues of privacy? Is the discussion within the community prevailingly expert and technical in style or is it more opinion based? For comparative purposes, the analysis was limited to articles published between 1st January 2010 and 31st April 2013. The basic unit of analysis is a 'statement', which we define as a part of a text (a sentence, a part of a sentence, or a whole paragraph) that expresses a particular 'idea', which means that it must also make sense to anyone who reads it outside the context of the article. Also, in order to designate a part of the text as a statement for the purposes of our study, it must also be possible to identify an actor making an argument about one of our selected topics. For the purpose of this study we obviously selected only those statements that referred to the subject of our study, and did so using the keywords 'CCTV cameras', '3D body scanners', or Stuxnet.

3.2 Coding

In the next step of the analysis, articles were coded using *Atlas.ti7*. Each statement was assigned a code in seven different categories of interest (see Table 1).

While not every statement could be assigned a code for every category, the codes in categories 1–4 were mandatory in order for a statement to be included in the analysis. Each of the three topics was coded according to a distinctive coding scheme. The coding schemes were designed on the basis of pre-tests and then revised 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

Four security-expert blogs written in English were selected for 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 reader turnout and its relevance to the objectives of the study.

Bemosa defines itself as an Airport Security Monitor. It is the corporate blog of Kirschenbaum Consulting, which provides professional security consulting services to airports, transport authorities, governments, security companies, and other high-risk organisations. The blog is written by Professor Alan Kirschenbaum, an expert in the area of disaster and crisis management and the initiator and coordinator of the EU-funded BEMOSA Project (www.bemosa.eu), a Europe-wide research project that has developed a behavioural model describing how in reality people make security decisions during a 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 from the perspective of the people it most immediately concerns: air traffic controllers, pilots, engineers, and managers at every level. The content is written by and for aviation professionals and has a space for reader comments. It is structured into categories listed in alphabetical order, and security is one of the categories. The blog is the 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 and of the four included in the analysis it has the most mysterious background, as it was not easy to find information on who runs the blog and what its purpose is. After contacting Mr. Dhillon Andrew Kannabhiran, the CEO of *Hack in the Box* (or *HITB*), we finally got the answer. Mr. Kannabhiran defines HITB as the community of organisers of the HITB Security Conference or the *HITB*SecConf series of community-backed, not-for-profit security conferences held annually in Kuala Lumpur, Malaysia, and Amsterdam, the Netherlands. The main aim of the *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 originally founded in London as an e-mail 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. The content was later merged in theregister.co.uk (Cullen 2003). As for readership, according to the Audit Bureau of Circulations, in 2012 it had more than 375,000 daily users (www.abc.org.uk, retrieved 24 October 2013). In May 2013, Alexa (a company providing commercial web traffic data) reported that the site ranked 4,012th in the world for its web traffic, down approximately 1,000 slots from the previous year. The content of *The Register* website/blog is divided into different sections. Channel Register covers computer business and trade news, including business press releases. News and articles on computer hardware and consumer electronics are covered by Reg Hardware. Reg Research is an in-depth resource on technologies and how they relate to business. The whole blog is divided into sections such as Networks, Science, Security, Jobs, Business, and Hardware.

The four selected blogs are clearly rather different in terms of their scope, who owns or operates them, and the type of articles or posts they offer. *Bemosa* and *Roger-Wilco* are highly specialised, narrow-topic weblogs on airport security and air traffic management, respectively. Both are backed by private consulting companies, so there is the possibility that the arguments presented may be skewed in favour of the business interests of the two consultancies. Furthermore, *Bemosa* is in fact a private blog of a single individual, Alan Kirschenbaum, who is accordingly also the sole author of all the posts. In contrast, *The Register* is more of a mass-impact, publisher-owned online magazine or newspaper covering a wide variety of topics connected with technology and related fields. It is one of the leading global websites for IT specialists. Most contributors are specialised journalists. By contrast, there is *HITB* – which is a blog operated by a non-profit company that organises security conferences in Malaysia and the Netherlands and which is endorsed by various Malaysian governmental and non-governmental agencies. It concentrates mostly on IT security issues. The posts are usually very short and borrowed from other online sources (e.g. blogs, IT news websites, online IT magazines, IT companies' newsletters) and often presented in abridged form. The posts are tagged by topic and source and are usually accompanied by a figure on the number of people who have read the post, which ranges from 1400 to 2000 per article.

3.3.2 The sample

To gather articles for analysis, all four blogs were searched for the following key words in English: 3D body scanners, Stuxnet, and CCTV cameras. From the results we selected only articles published between 1 January 2010 and 30 April 2013. The search returned a total of 345 articles, most of which – almost 80% of the search results – were on Stuxnet.

Table 2. Total sample – all articles returned in the search

Blog **Topic**	*The Register*	*HITB*	RW	*Bemosa*	**Total N**	**Total %**
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 some that turned out to be irrelevant to the objectives of the study. In most cases the reason was that the article included the key word, but was otherwise primarily referred to another topic. Once the relevant articles were selected, the total sample decreased to less than half its original size and comprised a total number of 150 articles. Again, the majority of articles referred to Stuxnet (almost 70%), CCTV cameras were the topic of nearly 20% of the articles, and about 11% referred to 3D body scanners.

Table 3. Total sample – selected relevant articles

Blog **Topic**	*The Register*	*HITB*	RW	*Bemosa*	**Total N**	**Total %**
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 the relevant articles were posted in 2010 and 2011. However, there is no significant evidence of any particular trend or peak occurring while the specific topics were being monitored in the blogs, nor is there evidence to suggest any correlations with other phenomena. There are differences though in the bias of topic coverage among blogs. Although the issue of Stuxnet was generally very dominant, we can see that *The Register* was the blog with the strongest topic 'bias'. 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 the other two topics were covered altogether by just 7 articles. The reason for this might be the blog's prevailing focus on IT issues. On the other hand, the other two blogs, *Roger-Wilco* and *Bemosa*, returned very small numbers of articles. RW returned two articles on the issue of 3D body scanners and *Bemosa* returned one article on CCTV cameras and two on 3D body scanners. This seems to be down to the highly specialised nature and narrow focus of those blogs, which deal mostly with issues of air traffic management and airport security. This is also why there was no Stuxnet coverage on these blogs as IT issues are logically not their concern.

Table 4. Relevant articles by 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 the articles varied. The majority of them were rather short and informative reports, often reprinted from other online magazines, blogs, and news agencies. They generally contained very limited or no analysis at all. Therefore, we had to be very careful about the articles selected for our sample. We used the method of purposeful sampling, and our main criterion was to select articles that would as much as possible fit the objectives of our study. In other words, we tried to choose from among the articles of topical relevance those which were somewhat longer, with the maximum possible density of actors and arguments relating to our objectives. We also attempted

to maintain a an even distribution of articles over time. However, this was not the primary aim for the reasons discussed above.

Table 5. Articles selected for analysis – final sample

Blog **Topic**	*The Register*	*HITB*	**RW**	*Bemosa*	**Total**
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 our analysis. The objective was to maintain an overall proportionality of topics and a relatively even number of relevant articles returned by each blog. On the other hand, in order to attain a more representative and biased final sample, some blogs and topics were over-represented and some under-represented compared to the distribution of relevant articles in the total sample. Table 6 shows the distribution of the 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 next section presents the findings of our qualitative textual analysis of the coverage and content of the discussions of CCTV cameras, Stuxnet and 3D body scanners in selected expert online blogs between 1 January 2010 and 30 April 2013. We will focus on the actors involved in the discussions, the exact topics of their discussions, the opinions of the actors, and how they justified their arguments. We will also examine patterns of framing the topics in particular blogs and possible differences. The analysis is structured by topic.

4.1 CCTV cameras

Generally, the main issue discussed in the articles we coded on CCTV cameras was the controversy over security and privacy and personal data storage. The six articles (out of a total of eight) from *The Register* blog were relatively long and most presented quite a high level of analysis. The main issues here were the surveillance of citizens in public areas and the various counter-terrorist and anti-crime security projects of the police and local authorities in the UK. A special focus was put on the ANPR system (Automated Number Plate Reader) used by the British police to monitor drivers. This system was mostly elicited criticism for the collection of personal data and its possible misuse. The same topic appeared in the *HITB* article, which was a very short report taken from another 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 the lessons to be learned from the experience of CCTV surveillance at airports, referring to a study done on airport security that claimed about a third of security employees regularly bend or even break rules and procedures when necessary. The article points out that such decisions are not made by individuals but as a group and in communication between security employees that runs 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 in the articles are the police (18%) and the civil society groups (18%), followed by state institutions (16.7%). The police was mentioned most often as the actor in control of CCTV surveillance tools and storing personal data and the actor criticised by various groups of civil society. Following from this, the representatives of state institutions (such as the British Home Office) were generally found to be defending or providing information about security provisions and the need for surveillance to ensure 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 were the most frequent theme coded from the statements (27%). The themes of surveillance and personal data protection (both 11.5%) represent the main controversy within the topic area, which logically is closely linked to security-related rules and regulations (9%) as the legal grounds for surveillance on the side of the state and the police. Public domain monitoring (7.7%) then constitutes a basic arena for such conduct. The blogs typically also provided information on new installations of CCTV cameras, followed by comments on the costs of such systems (6.4%) – for example, *'Local authority spending 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 November 2010) Definitive arguments, relatively informative and neutral, dominated among the coded statements. Among the statements on this topic we coded 50 as definitive, 2 as evaluative, and 2 as advocative, and the latter were both negative and

opposed to the use of CCTV cameras. As *The Register* writes, again quoting 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 November 2010)

The evaluative statements were also negative in tone. Representatives of civil society groups, Big Brother Watch, and No CCTV complained about the costs, inefficiency, and the controversy over the lawfulness of CCTV and its consistency with the principles of democracy. This example concerns ANPR systems, 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 June 2011)

The only positive statements identified came from police representatives defending the ANPR systems and claiming that the cameras are entirely lawful and highly efficient at targeting criminals and unsafe drivers.

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

Argumentation 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**

It was possible to identify justifications for the actors' arguments in 23% of the statements. The leading justifications were issues of efficiency, often the rather poor efficiency of CCTV, and issues of freedom/liberty, followed by costs. Another example for all, from the coded article cited above quoting the Big Brother Watch report, includes all the justifications at once, stressing costs and inefficiency:

'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 November 2010)

Table 10. Justifications used in arguments about 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 main use to the specialised focus of the two air traffic and airport security management blogs *Bemosa* and *Roger-Wilco*. This topic also provided the only instance when the RW blog entered our analysis, as the initial search returned only two RW articles, both exclusively on the topic of 3D body scanners. Similarly, the *Bemosa* blog covered the topic with two articles (out of the three returned in total in the initial search). The quality of the articles varied massively. *The Register* presented articles with high informational value and reasonable arguments expressed by a variety of actors, such as EU institutions, experts, and advocacy groups. On the other hand, the *HITB* posts were very short news reports dealing with rather minor issues, such as reporting on a woman whom a body scanner caught carrying 44 iPhones. The second *HITB* article pointed out that it was possible to avoid the full body screening by paying an official fee to TSA (Transport Security Administration), which seems to be an interesting topic. Nevertheless, the article contained no analysis or arguments and was informative only. The *Bemosa* blog

articles related directly to airport security and the role of the human factor, passengers and security staff, and their attitudes to security technology. Although the quality and expertise of these articles, there weren't many statements we could use for the objectives of our study. The *Roger-Wilco* articles, on the other hand, contained very strong arguments, generally criticising European institutions for inventing obstacles to prevent the introduction of full body scanning 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 in the debate were institutions (28%), followed by civil society groups, the scanners themselves (12.5%), and experts (12.5%). More specifically, the institutions mentioned were prevailingly EU institutions – the European Parliament, European Commission as a whole, EU Transport Commissioner, the European Economic and Social Committee. They were most often mentioned in relation to regulations concerning the introduction of 3D body scanners and the debate about their efficiency versus health risks and privacy protection issues. The expert category included mostly health and radiation experts judging the level of health risks. Civil society groups could be divided in two categories – those concerned with privacy issues, such as EPIC (Electronic Privacy Information Centre), and those concerned with health risk issues, such as 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 scanners were (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%). Freedom and terrorism appeared to be issues of little salience in the debate, which seems surprising in the case of terrorism, as 3D body scanners are in fact meant to be a counter-terrorist measure. Apparently, the debate was more concerned about the regulations of full-body scanning with respect to privacy and health. This can be demonstrated by such headlines 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 the *Roger-Wilco* blog and were the subject of criticism owing to an alleged neglect of security issues in favour of the rhetoric of human rights.

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

Argumentation 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 also coded numerous statements in which the direction of argument was negative. These statements emphasised health risks: for example, *'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 November 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'*; and 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 November 2011) Representatives of civil society groups 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 November 2011) A different example of statements with a negative direction/tone of argument are the articles on *Roger-Wilco* that negatively evaluated 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 will to arresting the one guy who is behind all the mischief.'* (*Roger-Wilco*, 12 January 2010) Although it was coded as a negative statement, it is obviously in fact strongly supportive of the idea of 3D body scanning. Another statement in support of scanners, which was 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 November 2011)

Table 14. Justifications used in arguments about 3D body scanners

Justification	**Frequency**	**%**
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 the justifications of arguments and the quotations from the articles show, the prevalent justification used in relation to body scanners were health issues, which were found in one-third of the statements that contained a justification. Privacy issues were the second most common justification (19%), followed by security (14.3%), and efficiency, freedom, and legality (9.5%). The issue of the costs of body scanning was not particularly significant in the debate.

4.3 Stuxnet

The Stuxnet worm was the most salient topic in the expert blog analysis. Almost 70% of the articles returned in the search were on this topic, which is really a very significant dominance of one topic. However, two of the blogs analysed did not return any articles related to Stuxnet. Not surprisingly, these were the highly specialised 'airport' blogs, *Roger-Wilco* and *Bemosa*, as this topic does not fit in their area of expertise. Of the other two blogs, *HITB* returned the most articles. Altogether, we coded 13 relevant articles from *HITB* and 11 articles from *The Register*. Although the quality of the *HITB* articles related to this topic could be said to be generally higher compared to the previous topics in terms of their level of expertise and informational value, the articles were still very short, were borrowed from other online sources, and did not offer any in-depth analysis or discussion of the 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. The *HITB* articles generally provided information about the Stuxnet worm's attack on Iran and presented news on Iran's official reactions to the attack and speculations about the origin and motives of the attack as well as about the states and organisations involved. The second theme (observed) could be defined as the future of cyber security in a post-Stuxnet world, which means possible future threats and their solutions.

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

Table 15. Actors and their country of 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							
TOTAL:	**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' background was often not explicitly mentioned; mostly they were computer security experts from private companies, computer scientists, or legal experts. On the other hand, the background of the second most frequent actor, state institutions, was often explicitly mentioned in the statements. We identified 15 cases of US state institutions as the actor, including the President of the United States, or 'senior US officials' and heads of government departments were mentioned. We also identified 6 cases of actors from Iranian state institutions, including the President of Iran, the head of Iran's atomic energy organisation, and other 'Iranian officials'. The other state institution actors were from Israel (3), China and Russia (1 each), and one supranational actor – the UN.

Table 16. Topics in articles on 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
TOTAL:	**169**	**100**

Cyber war was (coded as) the most frequent theme (14.2%), and Stuxnet itself was almost as common (13.6%), followed by the themes of an attack on Iran, the United States, or Israel, the development of Stuxnet by a state, and the deployment of or attack using Stuxnet. This illustrates very well what was already noted above in the general characterisation of the articles. Some articles were more informative and referred to the Stuxnet attack itself, the reactions of the international community and of Iran as the target of the attack, and the searching for the source of the attacks. For example: *'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 October 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 September 2012)

Other articles were devoted to the issues of international cyber security, the possibility of future cyber war, and the changing nature of international warfare. It was also possible to identify an emphasis on the need for a new legal framework, establishing what a cyber-attack is and if (or how) it is legal for a country to defend itself. For example:

> *'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 January 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 March 2013)

Table 17. Argumentation 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 tended to be objective and neutral. Furthermore, the state institutions as actors were not trying to be objective, but their statements represented their definitive standpoints. Most of the definitive statements with a negative direction/tone were expert statements disagreeing with the 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 January 2011)

Table 18. Justifications in relation to Stuxnet

Justification	Frequency	%
Efficiency	7	29.17
Defence	5	20.83
Pre-emptive strike	4	16.67
Security	3	12.50
Costs	2	8.33
Legality	2	8.33
Expert opinion	1	4.17
TOTAL:	**24**	**100**

Although this topic offered us the largest number of statements to code compared to the other two topics (100 statements), we were able to identify justifications in only 24 statements. Efficiency was the most frequent justification (29%), followed by defence (20.8%) and pre-emptive strikes (16.7%). The efficiency justification was mostly used in reference to the Stuxnet worm and the efficiency of its harmful effects. Defence and pre-emptive strikes were most frequently cited by legal experts as justifications for the right to carry out a cyber-attack for the purposes of defence:

> *'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 October 2010)

5 Summary: actors and argumentation strategies in expert blog articles referring to 3D body scanners, CCTV cameras and Stuxnet

There were major differences in the level of coverage given to particular topics in the blogs analysed. This applies to the bias of topics as well as to the overall number of relevant articles found in individual blogs. However, there was no evidence or tendency to link particular events and the content of the debates over time in the observed timespan, at least in the context of our analysis. Generally, the issue of Stuxnet was very dominant, with almost 70% of articles referring to this topic. CCTV was the topic of nearly 20% of the blog posts and about 11% of them dealt with 3D body scanners. *The Register* turned out to be relatively the most biased blog in terms of the distribution of

topics, although even there Stuxnet still dominated. The other three blogs analysed exhibited a rather narrow topical focus and concentrated mostly on issues of IT security, in the case of *Hack in the Box* (*HITB*), or exclusively on issues of air traffic management and airport security, in the cases of the *Roger-Wilco* and *Bemosa* blogs. The latter two blogs also returned a very small number of articles. Consequently, this poses certain limitations for applying a comparative perspective to the topics, as some blogs and topics were intentionally over-represented and some under-represented compared to the distribution of relevant articles in our total sample.

Table 19. Total sample – relevant articles

Blog **Topic**	*The Register*	*HITB*	RW	*Bemosa*	**Total N**	**Total %**
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 the content analysis of the expert blog discourse – 3D body scanners and CCTV cameras - we can observe a relative similarity of the actors making statements. In both cases, state institutions and civil society groups entered the debate the most. In the case of CCTV cameras, the police can also be included, since they can be regarded as a state institution of law-enforcement. As regards the 3D body scanners, institutions were by far the most frequent actor, prevailingly EU institutions – the European Parliament, European Commission, European committees, etc. The CCTV cameras debate, on the other hand, involved mostly national institutions, prevailingly British ones. These similarities seem to arise from the analogous core of the debate within these two topics, centred on the introduction or disposal of certain controversial security measures by national/European institutions towards citizens. Advocacy groups/civil society actors made statements responding to such behaviour. Numerous experts also entered the debate on 3D body scanners, most of them health and security professionals. The main points in the discourse on this topic 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 justification for a statement and was used mainly by experts and advocacy group workers judging the risks of 3D body scanning. This was followed by privacy

justifications, mostly given by civil society groups such as EPIC concerned about privacy issues.

Quite surprisingly, the more general issues of counter-terrorism protection and arising limitations to personal freedom were of little salience in the debate, even though 3D body scanners are in fact meant to be a counter-terrorist measure. However, in the expert blog discussion on CCTV cameras, the limitations to personal freedom connected with the surveillance of citizens in public areas and the protection of personal data were a major controversy. The security-related rules and regulations that constitute the legal grounds for surveillance on the side of the state and policy were then mostly criticised by representatives of civil society. The main justifications for such statements were the issues of poor efficiency, freedom/liberty, and costs. Representatives of state institutions and the police, on the other hand, provided information about or a defence of the CCTV security measures, arguing the great efficiency of CCTV and its positive effects on public security.

The Stuxnet topic was by far the most salient one in the expert blog analysis and was also significantly different from the two other topics. This blog community was particularly drawn to the topics of cyber security and hacking, since these are its main fields of interest. Given the global nature of the Stuxnet worm, the variety of actors identified was much higher and most frequently encompassed international experts, state institutions and the media. The exact background of the experts was left rather unspecified, while state institutions in particular were often identified with the nation they belong to; US state institutions were the most common, followed by Iranian and Israeli institutions. Generally, the articles analysed were either informative in nature, providing information about the Stuxnet attack on Iran, or focused on the issue of cyber-security challenges in the wake of the Stuxnet attacks. This entailed the three most frequent topics – cyber war, Stuxnet itself, and an attack on Iran. As regards the argumentation strategies used in the articles, the majority of coded statements were definitive and neutral, as was the case of statements across all three key topics studied. In the case of Stuxnet, experts, the main actors, tended to be objective and neutral, whilst state institutions, the second most important actor, presented definitive statements without trying to be objective. The justifications for these statements were efficiency in most cases, followed by defence and pre-emptive strikes. Efficiency referred mostly to the efficiency with which Stuxnet is able to cause harm and damage,

while defence and pre-emptive strikes were frequently used by legal experts to justify the right to carry out a cyber-attack for the purpose of defence.

Table 20. Argumentation strategies by direction of argument - total

Argumentation strategy	**Direction/Tone 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 for statements were found in approximately 25% of the statements analysed, with the exception of 3D body scanners, 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 the total of 173. However, a negative direction/tone of argument was more prevalent in some topics, such as 3D body scanners, where a negative direction/tone of argument was observed in approximately one-third of statements (both definitive, evaluative and advocative). These tended to be statements by representatives of civil society criticising the introduction of scanning. Statements with a positive direction/tone 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 presented the results of a qualitative textual analysis of the coverage and content of discussions of the topics of CCTV cameras, Stuxnet, and 3D body scanners in selected expert online blogs between 1 January 2010 and 30 April 2013. The analysis revealed that the domain of online expert blogs is a specific area that can differ considerably by its scope and nature from traditional print media. This is of course owing to their global online outreach and greater immediacy, interactivity, and interdependence with other sources. At the same time, blog writing does not need to adhere to the standards and practices of traditional media, such as presenting a balance of viewpoints or fact-based reporting. The significant differences between blogs in terms

of their scope, owners/operators, and the type of articles/posts published presents serious limitations for comparability and the possibility of bias in such analysis. Furthermore, we must bear in mind that apart from the differences in the target readers of particular blogs (e.g. the IT community, air-traffic professionals, or the general public), various relevant business interests may also come into play. Two of the blogs analysed (*Bemosa and Roger-Wilco*) are backed by private consulting companies, and this may skew the presentation of arguments in favour of the business interests of the two consultancies. On the other hand, there is also the mass-impact, publisher-owned online magazine and newspaper that is among the leading global websites for IT specialists and there is *HITB* – a blog operated by a non-profit company that organises security conferences in Malaysia and Netherlands and is endorsed by various Malaysian governmental and non-governmental agencies. It is obvious that business interests concerning the advertising, funding, and readership support will necessarily be very specific and may have an impact on the composition and character of the articles published. Nevertheless, we believe that the analysis may still serve as a valuable insight into the coverage and manner of coverage of our three security topics in a highly specific community. The analysis showed that, despite the fact that the selected blogs should contain expert opinions, the quality of the articles varies considerably. The most informative but also the least analytical blog was the *HITB* blog. It is merely an announcement blog, as it concentrates on short and media agency news from the security industry, with a focus on cyber security, but it provides only very limited analytical contributions. The *Bemosa* and *Roger-Wilco* blogs also have a very narrow topical focus, but they provided high-quality articles. Yet, due to their high specialisation, they offered only a limited amount of useful information for the objectives of our study. Only *The Register* blog proved to be a very sophisticated source of information and provided an in-depth discussion among readers.

To conclude, the results of our analysis in the selected time period and of the four expert blogs chosen showed that, in terms of saliency, the topic of the Stuxnet worm dominated significantly within the expert security blogs (accounting for about 70% of the relevant articles found). One reason for this could be that the focus of the prevailing and most fertile part of the blogosphere analysed is on IT issues (*HITB*, *The Register* – originally an IT technology news site, though currently more broadly oriented). Therefore, cyber security and hacking seem to be issues closest to their interests. CCTV cameras and 3D body scanners followed with 20% and 11%, respectively. Assessing the

nature of the discussion generally, although the blogs are supposed to be expert-oriented, the debate in the blogs was not very expert or technical. A large portion of the articles were short and informative. The articles with more in-depth analysis could then be described as more opinion-oriented, without dealing too much with specific technicalities. An exception would be one legal analysis of the possible implications for international law of the cyber-security debate in the wake of the Stuxnet attacks ('Stick Nuke Plants and Hospitals on No-go List Too - War Manual', *The Register*, 20 March 2013). It was also with respect to Stuxnet that questions of security were raised the most, referring to cyber-security challenges in a post-Stuxnet world and the possible threat of cyber war and the legal implications of all this. Concerning other two topics, CCTV cameras and 3D body scanners, the issue of privacy protection against security measures clearly dominated. Here more of a voice was given to experts and other actors criticising the security measures with arguments about privacy, human rights, health risks, costs, and inefficiency. On the other hand, we were also able to find support for security measures, particularly 3D body scanners, especially in the blogs focused on air-traffic management.

As we can see, although the 'blogosphere' is not a straightforward subject of analysis, research in this area can offer a valuable contribution to media content analysis, as the area of new social media is clearly 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,Traditional Sources Online and Political 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, Chicago, IL, September 2004.

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/)