The Xanadu of surveillance: Report on security perceptions in the British online media

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

Jessie Hronesova (ISASCR), Tristan Caulfield (ABDN), Petra Guasti (ISASCR)

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

Security Economics: Socio economics meets security

SECONOMICS Consortium

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

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESCHI Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	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.

INDEX

1. Introduction

Security has become a defining feature of contemporary public discourse, permeating the so-called 'war on terror', problems of everyday crime and disorder, the reconstruction of 'weak' or 'failed' states and the dramatic renaissance of the private security industry.
(Loader and Walker 2007).

In 1949 Eric Arthur Blair published a novel set in London describing a totalitarian state under the constant surveillance of the omnipresent and omnipotent "Big Brother." The author presented his vision of the world in 1984 as a totalitarian community. He is better known by his pseudonym, George Orwell, and his perennial bestseller, "1984," has once more enjoyed a renaissance in 2013. Orwell's popularity in the past year is not a mere coincidence. A series of high-profile cases related to leakages of top secret information from the intelligence services have shaken public confidence in the legality national governments' security practices. The information revealed by Chelsea Manning, Edward Snowden, and Julian Assange has come to represent the secretive and increasing state intrusions into private lives, intrusions which are justified by the war on terror and carried out under the aegis of counter-terrorism. The charges raised against these three now prominent figures have intensified debates about the extent of powers a state can and should exert over its citizens. The question of who controls the controllers has emerged once more. The negative implications of security, which had previously been neglected, have slowly come to the forefront of comprehensive analyses of state security and risk management.

Social sciences have produced a plethora of security and risk related literature, but the field of enquiry and practice is by no means novel. The term "risk" was in fact coined in the 16th century by western sailors navigating worlds unknown to them. They used the term "risk" to describe dangerous waters (Denney 2005, 12). In pre-modern times, risks and dangers were of great state concern. Disease, war, epidemic, and famine were all considered dangers, and later whole social classes came to be referred to as dangerous. Risk gained a new meaning during the Industrial Revolution and with the advance of modernity and modern commerce and business where it became closely linked to uncertainty about the future. In the past certain ethnic or national groups and religious communities were portrayed as presenting a danger or threat to other nations. In the beginning of the 20th century, such notions were also applied to anarchists and Jews, and later to communists and socialists. In the 1970s, even young people came to be portrayed as a "dangerous group," a "mugging class," because so many youth were involved in criminal cases. (Denney 2005, 8). Since the late 1980s, topics such as nuclear radiation, chemical waste, and weapons, including the use of biological weapons, have begun to constitute a new post-modern set of dangers and risks that are quite unlike in the risks conceived in any previous era. In recent decades, international terrorism and organized crime came to replace the threats posed by violent, non-conformist groups that posed a threat to the general public. Today's post-modern time faces yet another series of threats and risks which are associated with technological advances and the vast potential of

cyberspace. It is thus not surprising that already in 1995, 1.5 million people in the United Kingdom were employed in what could be termed "the risk industry" (Denney 2005, 1), i.e. activities and services related to reducing and procuring security for the public.

In 1992 Ulrich Beck, one of the most influential authors in the field of risk theory, coined the term "Risk Society" to describe these new dangers and society's perception of them. He argued that we live in a society driven by "unsafety." The Internet and other modern technologies have created a space for new kinds of global crime which are not limited by physical boundaries. Beck grounds his analysis in the recent technological changes of our post-modern and post-traditional world, enumerating an endless list of potential risks and threats we face on a daily basis. Although pre-modern societies lacked the complexity of current risks, he argues that perceptions of the threat of hell, demons, plague, and the like can be compared to our perceptions of the destructiveness of nuclear war. Furthermore, he divides risk into two categories. Manufactured risks grow from the threats created by technology and science. External risks, on the other hand, spring from the natural world. "Risk," he notes, "may be defined as a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself" (Beck 1992, 21). At an analytical level, risk assessment is "the process of identifying hazards which may cause an accident, disaster or harm" (Manthorpe cited in Denney 2005, 18). Since security is the process of reducing the number of risks, the theory of risk management is extremely relevant for this research.

Beck's Risk Society is a useful starting point for the study of perceptions of security in post-modern times and the study of relations between the state and the people in terms of safety and privacy. If security is one of the fundamental "goods" ensured by the state (Loader and Walker 2007), at what costs are security measures still justifiable? Shouldn't respect for privacy and the right for information be just as fundamental and observed as the provision of security? It has been established that people are willing to give up a certain amount of their privacy in exchange for security. This is most notably demonstrated in the case of the British people, who are irritated by, yet willing to accept the ubiquitous presence of CCTV. However, full body scanners, which effectively strip a person naked in digitalized 3D images, borders on what is acceptable for human dignity for many, especially for the vast number of religious minorities in Britain. The dilemma of what is the acceptable trade-off between privacy and security thus arises. Lastly, in terms of global politics, the 21st century will certainly remain a century of wars; however, a new type of war has emerged, which is also related to the technological revolution of the last 20 years.

Cyber wars and hacking are effective, yet non-violent attacks that seek to paralyze a country or some of its infrastructure and capacity.[1] This was clearly evident in the 2010 Stuxnet attack on Iran. The malware Stuxnet was a worm released to sabotage the Iranian nuclear programme by targeting its

---

[1]"Stuxnet: Computer worm opens new era of warfare", CBS News, 1 July 2012, http://www.cbsnews.com/8301-18560_162-57460009/stuxnet-computer-worm-opens-new-era-of-warfare/

critical industrial infrastructure in 2010. Unlike its forerunners, Stuxnet was designed to achieve effects in the physical world and challenged the belief that network defences can protect facilities from software vulnerabilities. More importantly, the malware has started a new arms race and raised questions about the safety of national critical infrastructure (see Collins and McCombie 2012). The news of the cyber-attack also raised questions about state power and the limited voice of citizens' in international affairs. Though a certain level of secrecy is necessary, it is important to debate what degree of secrecy is and is not in the interest of citizens.

These questions have not failed to interest the world media and the general public. As Barndard-Wills noted, the "the trope of Big Brother and a number of variants ("Orwellian," "1984," etc.) are ubiquitous in the media discourse about surveillance" (Barnard-Wills 2011, 559). The growing and widening opportunity for expressing one's views in public arenas online has also diversified the group of people expressing such views. Stories about security have been steady and constant in the British press. Since the London bombings of 7 July 2005 (henceforth referred to as "7/7"), political discourse has been amplified by what Hoskins and O'Loughlin (2010) call "security journalism." Traditional and new media have been instrumental in understanding the perceptions and acceptance of surveillance systems (see especially Gates and Magnet 2007). By studying the news and discourse used in the media, one can understand how anxieties can become pervasive in society, as discussed by Monahan (2011) in his analysis of media as a force for creating both (subjective or imaginary) senses of safety and insecurity. Despite this power, the public is not merely some blind follower of the media. In fact, "audience members alternatively accept, ignore, and reinterpret the dominant frames offered by the media" (Neuman 1992, 62). The interaction between the state, the media, and the public is thus a fruitful ground for analysis.

This paper operationalizes the concept of risk, framing it in terms of the dangers and threats which affect security concerns in the UK. Furthermore, we focus on risks that are a product of modern science and society. Furthermore, we analyze security through a constructivist prism mediated by social and cultural processes and realities. Epistemologically, we do not analyze security as "real" or "objective," but as a constructed phenomenon. We study advanced technology and their consequences, such as cyber warfare. We also study security technology in particular, such as closed circuit TV systems and body scanners.

As a result of this focus, two institutions come into play: the state and the media. Due to its power, the state plays the key role in maintaining and increasing the security of its citizens through various security measures. But the understanding and acceptance of these measures is mediated by newspapers and broadcasters. Since there is currently little exhaustive research on how the media considers perceptions of security in their reporting, this paper hopes to make a substative contribution to the growing field of security studies.

Motivated by the changing nature of security-related issues, the expanding

role of online journalism, and the importance of studying security as a topic within interdisciplinary and policy-relevant research projects, this report represents one part of a cross-national research project titled SECONOMICS: "Socio-Economics meets Security".[2] The broad aims of the project are to identify security threats in transport and critical infrastructure. This case study of the UK is the product of a Graduate School organized by the Academy of Sciences in Prague (13-18 May 2013), which focused on security topics and the media's perception of them. Qualitative social science approaches were the main methods taught and applied during the Summer School. In order to produce several national reports of comparable quality, the Summer School provided extensive training in the qualitative coding of national newspaper articles on three selected topics. These topics, CCTV, 3D Body Scanners, and Stuxnet are three common themes in contemporary media that also represent broader global trends. Closed circuit camera systems are a good window into the trade-off between security and privacy. Full body scanners pose similar dilemmas, but also challenge some concepts of human dignity. Finally, Stuxnet touches upon much broader questions of national security and the limits of cyber-war, as well as questions about how much one state may impinge on another's sovereignty through new, non-violent technological means.

This paper analyses the news media coverage of the three selected security topics through a content analysis of the online versions of two UK newspapers: *The Guardian* and *The Daily Telegraph*. It focuses on the representation and evaluation of CCTV, 3D Body scanners, and Stuxnet in mass media and examines the diversity of attitudes along politically motivated media divisions. As a national report on the United Kingdom, it aims to answer some overarching questions of the SECONOMICS project. In particular, it examines the perceived trade-offs between security and privacy. It further considers whether media coverage of terrorism has made the public more sensitive to security issues, and discusses the various threats presented in the media. Lastly, it also tackles the topic of new technologies and their influence on security and the new, post-modern risks which result, in line with Ulrich Beck's notions of the "Risk Society" (1992). This national report makes use of qualitative content analysis methods, researching news media coverage in the period from January 2010 to May 2013.

The present national case study of the United Kingdom, divided into six sections, provides contextual, methodological, and analytical content. Section 2 offers some necessary background information about the latest political developments in the UK, as well as an overview of the British media landscape. It discusses security policies in the United Kingdom in the past decades, and the British national experience with violent terrorist attacks, which have determined its current policies. It further provides some necessary background on the nature and role of the British national press and media as the principle means of political communication. Section 3 is dedicated to the applied qualitative methods and explains in detail the sample selection. Section 4 provides the actual analysis of the selected

---

[2]For the official website see http://seconomicsproject.eu/.

articles, divided by the three selected topics. The last two sections provide succinct summaries and conclusions for the British case. The overarching findings of this research aim to contribute to the fields of security studies and communication studies by their original and focussed analysis of the three specific topics. As this is just a component of the SECONOMICS project, this report provides and in-depth analysis of the British case only, and should be understood and interpreted alongside the other national cases presented in the full outcome of this project. However, the British case is especially relevant for an analysis of the discrepancies and similarities between EU and US security policies.

2. Framing the study: security, politics, and media in the UK

2.1. Security and Politics in the UK

*The security of our nation is the first duty of
government. It is the foundation of our freedom and our
prosperity
(Cabinet Office 2010, 9).*

The new British Coalition Government led by David Cameron gave security the highest national priority in 2010 and created a new National Security Council. Like the citation from the Cabinet Office's 2010 statement, we conceptualize security as a public good necessary for the functioning of a developed democratic system; both at the individual and national level (cf. Loader and Walker 2007). Security as a public good procured by the state is critical to the attainment of people's self-actualization. Citizens can invest their resources and energy into their private, professional, and economic goals only if they are certain of their security (Ericson 2007), and not threatened by their fellow citizens. Loader and Walker (2007, 8) argue that security is a "'thick public' good, one whose production has irreducibly social dimensions, a good that helps to constitute the very idea of 'publicness.' Security, in other words, is simultaneously the producer and product of forms of trust and abstract solidarity between intimates and strangers that are [a] prerequisite to democratic political communities." The idea of security is thus conceptualized on two levels – the individual (public) and the national (state) – which are connected by the public media sphere. For a citizen, the feeling of safety and certainty creates a notion of security. Similarly, state security as a good is procured by national institutions (police and intelligence services) and involves not only delivering the feeling of safety, but also physical protection of national borders, territory, and a state's citizens from any external threat.

By all available indicators, the United Kingdom is a relatively robust, full-fledged democracy with highly developed governance structures.[3] The OECD 2013 Economic Survey provided some important quantitative indicators about the level of physical, economic and social security of British citizens. According to their findings, 71% of people feel safe walking alone at night, which is above the OECD average of 67%.[4] OECD national surveys are compared to other countries, assigning the lowest score 1 to states with poor services and 10 with the highest. The United Kingdom scored 9.6 on the variable "Safety," but only 7 on the variable "Life Satisfaction." These findings are interesting especially in view of the recent historical experience with terrorism and separatist groups. Given the economic crunch of the past five years, life satisfaction can be interpreted in economic, rather than societal terms. Overall, the OECD findings confirm the results of similar indicators, which consider Britain to be one of the safest countries in the

---

[3]See, for example, the State Fragility Index, Freedom House Index, Economist Index, and Polity IV indices.

[4]See *OECD Better Life Index. United Kingdom*. 2013. OECD, accessed on 28 September 2013, http://www.oecdbetterlifeindex.org/countries/united-kingdom/

world.

This safety correlates with the fact that Britain is the most watched country in the world. According to July 2013 data, Britain has one CCTV camera for every 11 people.[5] As early as 2004, the Information Commissioner Richard Thomas warned that UK was "sleepwalking into a surveillance society"[6]. The British Security Industry Authority (BSIA) reported that a staggering 5.9 million closed-circuit television cameras had been installed in the country since the 1980s.[7] Although 98% of these devices have been installed by private companies or for private usage, the level of surveillance in the UK is truly unprecedented. Not even New York and Chicago, which have significantly higher crime rates than any city in the UK, can compete with the level of surveillance in London. In a recent CNN article, London was titled "the Xanadu of winking, digital eyes"[8], again referring to the sheer number of monitoring devices. Britain has become the paradigmatic example of a "CCTV state" (see Hier, Walby, and Greenberg 2006) where surveillance is now taken for granted as part of daily life.

Surveillance can be, according to David Lyon (2002), evaluated according to a spectrum from "care" to "control" – from watching over society for purposes of protection, to scrutinizing people's behaviour for the enforcement of discipline and order. Surveillance is in his view the systematic monitoring of people and groups in order to regulate their behaviour, for example through CCTV.

Meanwhile, in his analysis of media practices reporting surveillance, Barnard-Wills found that there are two lines of argumentation presented by the press. The first is framed around a discourse of "appropriate surveillance," which argues that surveillance can prevent crime, terrorism, and preserve national security. The second line of argument, which he calls a "discourse of inappropriate surveillance," utilizes discourses like privacy, "Big Brother," and personal liberty (see Barnard-Wills 2011). Surveillance has serious implications in regards to human rights and privacy. CCTV by its very nature undermines citizens' fundamental right to privacy as affirmed in Article 8 of the European Convention on Human Rights. Some CCTV devices even record sound, further increasing their invasiveness (Schlehahn et al. 2013, 14). Although the British public is very sensitive to issues of privacy, according to several studies analyzed by Barnard-Wills, the press has been very positive about the installation of CCTV and often instrumental in the success of surveillance. A good example of this is the reporting about the July 7, 2005 London bombers and the Soho pub bomber in 1999 (Ibid.).

---

[5]"5.9. million CCTV cameras in the UK," 11 July 2013, *BBC,* accessed on 28 August 2013, online at: http://www.bbc.co.uk/newsround/23279409

[6]"Big Brother: What it really means in Britain today", 15 January 2007, *Independent.co.uk*, accessed on 28 August 2013, online at: http://www.independent.co.uk/news/uk/politics/big-brother-what-it-really-means-in-britain-today-432200.html

[7]"5.9. million CCTV cameras in the UK," 11 July 2013, *BBC,* accessed on 28 August 2013, online at: http://www.bbc.co.uk/newsround/23279409

[8]Keith Proctor. 13 April 2013, "The great surveillance boom," *CNN Magazine*, accessed on 28 August 2013, online at: http://management.fortune.cnn.com/2013/04/26/video-surveillance-boston-bombings/

The general British attitude to CCTV has changed over the years, though. From the initial outrage at living in "one nation under CCTV," watched by the Orwellian "Big Brother," CCTV has become a point of ridicule, mockery, and humour. The urban sign "Smile, you are on CCTV" has too many Britons become a daily "fact of life" (see Goold, Loader, and Thumala 2013). Moreover, decreasing crime statistics seemingly support the CCTV trend, although a clear positive correlation has not been proven in any existing research (see Reid and Andresen 2012). According to the UK Peace Index 2013 report, both crime and homicide rates have fallen significantly in the UK.[9] In England and Wales, the rate of first-time offenders has fallen by nearly half since 2007. The report lists "Changes in police practices and technological improvements" as one of the four potential causes for these changes in criminality rates. CCTV can function as a deterrence mechanism, but it can also help solve crimes. In 2009 the majority of Scotland Yard murder cases used CCTV footage as evidence.

Both the 7 July 2005 London bombing, in which the Luton railway station provided images of the perpetrators, and the aborted attack on 21 July 2005, where the police were able to rapidly issue images of the alleged culprits captured on buses, tube trains and stations, demonstrated the importance of CCTV images was demonstrated both for London bombing in 2005, where images.[10] Many high-profile cases were solved with the assistance of CCTV or other surveillance video. Despite these benefits, the ubiquitous nature of surveillance in Britain poses a threat to human rights – "right to be left alone" – and to private lives (Joinson 2013, 120). Some Muslim communities, in particular in Birmingham, have voiced their disagreement with the installation of CCTV cameras around their neighbourhoods without their consent (Choudhury and Fenwick 2011, 173). The reaction was quite contentious:

> There were angry public meetings in the city last week, after The Guardian disclosed the cameras were paid for by the Terrorism and Allied Matters (Tam) fund, administered by the Association of Chief Police Officers. Its grants are for projects that "deter or prevent terrorism or help to prosecute those responsible". Police sources said the initiative was the first of its kind in the UK that sought to monitor a population seen as "at risk" of extremism (Lewis 2010).

The scheme was eventually scrapped, and the cameras removed, but the attempt shows a response to domestic fears. Though accepted as an inseparable part of life in Britain, Janus-faced CCTV often raises public concern about state infringement of civil rights.

The somewhat relaxed attitude of the British public to surveillance can be partially explained by security concerns related to Britain's historical experience with the terrorism of the Irish Republican Army (IRA) and recent

---

[9]"UK Peace Index, Exploring the fabric of peace in the UK from 2003 to 2012." 2013. *The Institute for Economics and Peace (IEP),* accessed on 28 September 2013, online at: http://www.visionofhumanity.org/pdf/ukpi/UK_Peace_Index_report_2013.pdf

[10]Kate Dailey, "The rise of CCTV surveillance in the US", *BBC News Magazine*, 18 April 2013, accessed on 28 August 2013, online at: http://www.bbc.co.uk/news/magazine-22274770

terrorist attacks in London. From the late 1960s onwards, IRA terrorist acts have cost over 3000 lives, with the highest death tolls in Birmingham and Guilford in 1974 (Breau, Livingstone, and O'Connell 2002, 1). Violent clashes over Northern Ireland and its separation or unity with the United Kingdom have played major roles in drafting security policies in the UK. The Good Friday Agreement of 1998 between the British and Irish governments put an end to direct violent terrorist acts in England. However, a series of new terrorist threats emerged in the 1990s and 2000s. With the advent of a new Labour government in 1997, the British political landscape has undergone some major security reforms. In 2000 a new Terrorism Act went into effect. It repealed previous terrorist legislation mainly directed at Irish nationalists. Among other things, the 2000 Act allows people to be arrested in the UK for inciting terrorism abroad and broadens the definition of terrorism "to include the use or threat of action, designed to influence the government or intimidate a section of the public, for a political, religious or ideological cause where this action or threat of action involves violence or damage to property or creates a serious risk to the health or safety of a section of the public" (Ibid., 3). The 2000 Terrorism Acts has created the backbone of what can be considered one of the strictest anti-terrorism measures in the world (together with the US) (see Hewitt 2008).

The response of the United Kingdom to the events of September 11 has taken several forms. In addition to the support of the US military action in Afghanistan, the Labour government of Tony Blair introduced new anti-terrorist legislation and prioritized the prevention of terrorism in the work of its security and intelligence agencies. The 2001 Anti-Terrorism, Crime, and Security Act includes serious restrictions on rights, such as privacy and liberty, and reintroduces internment without trial to UK law. Despite increased security measures and the new legislation, the United Kingdom experienced a terrorist attack on its territory in 2005. On 7 July 2005, four bombs detonated across the central London transport system, killing 53 people and injuring over 700.[11] *Al Qaeda* claimed partial responsibility for the attacks, but the actual extent of its involvement remains unclear. The Blair government reacted by yet again outlining new anti-terrorism measures and by reaching out to Muslim communities in the UK. The new 2005 Prevention of Terrorism Act instituted restrictions imposed by the Home Secretary on anyone seen guilty of a "terrorism-related" activity. The deportation of foreign citizens was included in the act as a prevention measure and penalty (H. Office 2009). In the wake of the attacks and the growing public concern for tough security measures bordering on breaches of human rights, in 2005 the Director General of MI5 stated:

> I think that this is a central dilemma, how to protect our citizens within the rule of law when intelligence does not amount to clear cut evidence and when it is fragile. We also, of course, and I repeat in both our countries and within the EU value civil liberties and wish to do nothing to damage these hard-fought for rights. But the world has changed and there needs to be a debate on whether some erosion of what we all value may be necessary to

---

[11]For a media coverage of the events, see the multimedia section in *The Guardian*: "7 July Attacks in London", *The Guardian*, accessed on 28 September 2013, online at: http://www.theguardian.com/uk/july7

> improve the chances of our citizens not being blown apart as they go about their daily lives.[12]

Her speech tackled the main dilemma of security studies, i.e. the balance between protection and safety on the one hand, and respect for human and civil rights, together with privacy, on the other. In 2006, Amnesty International criticised the UK government for "sacrificing human rights for state security" (Beckman 2013, 51). The trend towards strict measures and zero tolerance of any extremist views, which could potentially lead to violent terrorist acts, was only reinforced in the latest legislation – the Terrorism Act of 2006, the Counter-Terrorism Act of 2008, and the Terrorism Prevention and Investigation Measures Act of 2011. These acts punish even support for terrorist acts and greatly expand state powers to monitor its citizens through access to private information and taping personal conversations. Moreover, any suspect of terrorism can be detained for 28 days without any legal consequences if charges prove unsubstantiated.

The events of 9/11 and 7/7 also led to increased security measures in transportation. In addition to metal detectors and greater restrictions on items permissible on-board, the UK Home Office and the US Transportation Security Administration introduced full body scanners in 2009 as a response to the failed attempt to blow up a Northwest Airlines aircraft by a Nigerian man who had sown the explosives into his clothing. The scanners are hoped to increase security in aviation by detecting liquids and non-metallic objects. Manchester and Heathrow airports were the first to introduce millimetre wave and backscatter scanning devices, while the remaining UK airports awaited a clear decision on the legal controversies surrounding their application. The scanners are regarded as potentially hazardous to human health, as the most commonly used body scanner technologies utilize millimetre waves, X-ray backscatter, and X-ray transmission imagery, which produce high doses of radiation. Moreover, some tests and studies presented equivocal results regarding their effectiveness while revealing a generally high rate of false alarms (Schlehahn et al. 2013, vi). The European Parliament even launched an open debate on body scanners and the operation of intelligence services in the context of counter-terrorism strategies in 2010.[13] While acknowledging the usefulness of the body scanners in the protection of passengers (since commercial aircraft continue to be a fundamental target for terrorists), the EU has not reached a consensus on their application. Concerns remain about whether the scanners are compatible with people's right to privacy and intimacy. Furthermore, the Commission issued a regulation in 2011 prohibiting the use of body scanners which utilise ionising radiation in the EU (Schlehahn et al. 2013, 62).

---

[12]"The International Terrorist Threat and the Dilemmas in Countering it." 1 September 2005. Speech by The Director General of The Security Service, Dame Eliza Manningham-Buller, delivered in The Hague, Netherlands, accessed on 28 September 2013, online at: http://hawk.ethz.ch/serviceengine/Files/ISN/90880/ipriadoc_doc/b0b57b89-708e-4328-94b5-d95f967f38b8/en/2014_ManninghamBullerA.pdf

[13]"Body scanners - Operation of intelligence services in the context of counter-terrorism strategies (debate)." 10 February 2010. *European Parliament,* accessed on 28 September 2013, online at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20100210+ITEM-014+DOC+XML+V0//EN

Furthermore, body scanners have been criticised for violating human rights, specifically privacy, human dignity, and data protection (Ibid., 63). In the UK a public inquiry established that 80% of British citizens reject the UK's body scanning at airports. In addition, existing cost-benefit analyses suggest that body scanners are not an effective investment for fighting terrorism (Stewart and Mueller 2011). Such results have been largely ignored and plans to buy more scanners for Stansted, Glasgow, Edinburgh, London City, and Birmingham have gone forward as body scanners have gradually become compulsory for all UK airports. More importantly, concerns have been raised whether counter-terrorism laws and policies have been targeting and alienating Muslims, sustaining and feeding terrorism. To many members of the Muslim religious community, full body images are humiliating and imping upon their behaviour codes of modesty (Choudhury and Fenwick 2011, 159). The existing research on the use of body scanners suggests that there is an overall lack of publicly available information with regards to the use of body images produced by the scanners (Ibid.).

CCTV and the 3D Body scanners are technologies used to prevent traditional crime and modern terrorism, as well as identify perpetrators. However, another area in the field of security studies, criminology and counter-terrorism, has become salient in the discourse of one modern security risk, cyber-crime. Cyber-crime has become a common high-volume crime in the UK, which often outnumbers burglary and robbery cases (see Wall and Williams 2013). There has been a tenfold increase in malware attacks in the period from 2008 to 2009. As many as 60,000 attacks were registered each day in the UK in 2009 (Cornish et al. 2011, 6). Cyber-crime uses information systems and technology to commit extortion, identity theft, espionage, or even achieve the paralysation of critical infrastructure. Among many others, in June 2010 a worm was developed by the USA and Israel to interfere with uranium enrichment in the Iranian nuclear facility at Natanz, which opened a new era in cyber warfare. Stuxnet was designed as a highly sophisticated malware, which targeted a very particular section of the Iranian nuclear facility (see Collins and McCombie 2012).

In response to the media reports about the attack the British government called for international coordination on cyber security strategies while securing an advantage in cyberspace (Farwell and Rohozinski 2011, 31). The reason why Stuxnet has shaken the public views about cyber security is that it was unprecedented in its scope and effectiveness. It is a "sophisticated computer program designed to penetrate and establish control over remote systems in a quasi-autonomous fashion" (Farwell and Rohozinski 2011, 24). It has also shown that cyberspace is less costly and risky to use against enemies than traditional military measures. In response to these developments, the British Government released the National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) in October 2010 and devoted over £650 million to increase cyber security (Cornish et al. 2011, viii). However, a clear roadmap which would structure best practices and transparency in cyber security is still under development.

The British historical experience with domestic separatism and violent attacks, combined with the most recent terrorist attacks on its territory, has shaped current British security policies. Surveillance and improved transportation security measures have been top governmental priorities, especially since the 9/11 attacks in New York City and the 7/7 attacks in London. The current trend towards installing more monitoring systems and scanning devices in airports has prioritized security at the cost of human rights, intimacy and privacy. The "one nation under CCTV" slogan has been a very succinct mockery of the excessive use of monitoring in the UK. Their installation in elevators and even dressing rooms often leads to controversies about the use of such footage, similar to debates about whether the benefits of the use of 3D body scanners outweigh the social and ethical costs of their usage. In addition, some groups have been particular targets of increased security measures in public transportation, which could potentially engender further radicalization of the growing immigrant communities in the UK. In cyber space the UK has not pioneered any path-breaking research or technological development, as cyber security has still not been duly appreciated as a principle security priority. However, new strategies and approaches to promote best cyber practices are underway and it can be expected that with the rise of cyber-attacks, cyber security will move up the list of government priorities in the next decades.

2.2. British Media Landscape

The Daily Mirror *is read by people who think they run the country;*
The Guardian *is read by people who think they ought to run the
country;* The Times *is read by people who actually do run the
country;*
the Daily Mail *is read by the wives of the people who run the
country;*
the Financial Times *is read by people who own the country;*
The Morning Star *is read by people who think the country ought to
be run by another country; and*
The Daily Telegraph *is read by people who think it is.*
(Yes Prime Minister, Conflict of Interest, BBC 1986,
cited in Temple 2008, 190)

The British press, that "feral beast," as Tony Blair famously called it, claims one of the oldest traditions of journalism in the world, with the first British daily published in 1702 (Temple 2008, i). Already in the 18th century, the United Kingdom pioneered a new approach to public communication with a greater territorial scope and a new type of public messages. The German sociologist Jurgen Habermas saw Britain as the first country to develop what he called the "public sphere," i.e. a "realm of our social life in which something approaching public opinion can be formed" (Habermas, Lennox, and Lennox 1974, 49). In particular, to him newspapers in Britain attained their modern function of not only reporting about events but also about creating and forming public opinions by the exposure of individual views in the public realm (Ibid). Newspapers in Britain thus started early on (and earlier than elsewhere) to play an important role in public opinion making processes, quickly earning the title of a *Fourth Estate* from Edmund Burke. Yet their primary function is to inform, to educate, to provide a platform for the formation of political discourse, to channel political viewpoints, and to hold authority accountable (in a watchdog role) (Ibid., p.19). The above-cited mockery of the political and societal divisions of the readership of the press is a case in point. In order to perform these functions, which are so crucial for any viable democratic system, the media needs to be accessible to all citizens and they need to be free from political and economic constraints. These and other aspects of how media function in the UK are discussed below.

Historically, there are three categories of newspapers published in the UK. First are broadsheets, which are more serious, quality publications. Their name derives from their original large, wide format, which has now shrunk to match their smaller counterparts. Second are middle-market papers, which offer a combination of serious news and entertainment, but focus on information rather than analysis. Third are tabloids, which emphasize entertainment and are often referred to as trash news or "red tops" (Temple 2008, 86-92). There are 23 national newspapers, including the Sunday editions, in all three categories. In addition, there are also hundreds of regional and local newspapers (*OfCom* data from 2013). It is general knowledge among the readers which part of the political spectrum these

newspapers represent. *The Daily Telegraph, The Sunday Telegraph, The Times,* and *The Sunday Times* lean to the right. *The Guardian, The Observer* (the Sunday paper of *The Guardian*), *The Independent, The Independent on Sunday* and *i,* a paper aimed at younger readers and commuters, published by the owners of *The Independent,* lean to the left. *The Financial Times* is politically centrist, but economically liberal. The middle-market tabloids, *Daily Mail, The Mail on Sunday, Daily Express,* and *Sunday Express* are all right-leaning. The tabloid papers *The Sun, The Sun on Sunday* (the replacement for *News of the World*), *Daily Star,* and *Daily Star Sunday* are right-leaning. *Daily Mirror, Sunday Mirror,* and *The People* are left-leaning. The political slant of the newspapers does not always determine which party they back in elections. For example, *The Sun* backed Tony Blair's New Labour, became critical of Gordon Brown, Blair's successor, and eventually backed David Cameron and the Conservatives in 2010.

Regarding journalistic quality of the published news, there is a great diversity in journalistic principles and editorial policies. Alan Rusbridger, the Editor of *The Guardian,* maintains that the paper upholds the dictum of "Comment is free, fact is sacred" and that the paper "took a decision not to follow the fashion of blurring the lines between fact and comment".[14] Regarding the political and editorial influence of owners on the content of their papers, it seems unequivocal that owners exert serious influence over what is and is not permissible to be published. There is now a vast array of literature analysing how media frame and report events and how laden they are with subjective value judgments and opinions, which are often in line with their ownership (see McNair 2013). According to the House of Lords enquiry, Rupert Murdoch admitted that in his media outlets he did have "editorial control on major issues"[15]. *The Sunday Times* openly described how Mr. Murdoch decided to switch the allegiance of his two Tory tabloids *The Sun* and the *News of the World* to the Labour Party during the 1997 general election.[16] Public broadcasters such as the BBC are controlled by their trusts, which can also steer the content of their broadcasting activities.

Scores for media trustworthiness in the UK vary. According to *OfCom,* most TV news viewers and radio listeners rate their sources highly in terms of trustworthiness.[17] The BBC in particular scores very highly. Ratings are more varied for newspaper readers, with broadsheet readers rating their newspapers particularly highly as being trustworthy. Online users rate websites in more differentiated ways than other platforms as there is more scope for diversity and rating often applies to technological features as

[14]"The ownership of the news. Volume I: Report (HL Paper 122–I)", 27 June 2008, House of Lords, Select Committee on Communications - 1st Report of Session 2007–08, accessed on 15 September 2013, online at:
http://www.publications.parliament.uk/pa/ld200708/ldselect/ldcomuni/122/122i.pdf, p. 38.
[15]Ibid., p. 33.
[16]"Communications Market Report 2013", 1 August 2013, *OfCom*, accessed on 18 September 2013, online at: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr13/2013_UK_CMR.pdf, p. 111.
[17]Ibid.

well.[18] These findings are quite interesting especially since the 2013 MORI poll suggests that 72% people in the UK have no trust in journalists, which ranks this profession as the third least-trusted after politicians and bankers.[19] This might be caused by the discrepancy by the actual profession – a journalist portrayed as an aggressive and unscrupulous scandal seeker – and the respect entrusted into traditional broadcasters such as the British Broadcasting Company (BBC).

With the advent of new online media types and technological advances, journalism has undergone several important transformations. Traditional media has been under considerable pressure across the world as newspapers, television, and radio have been losing revenue to the Internet. New electronic means of distribution have resulted in a proliferation of news sources and the traditional print press has lost its dominant position in the news media market, which has led to financial difficulties. The overall number of adults reading at least one of the top ten national daily newspapers on an average day in the UK has been reduced by 19% between 1992 and 2006 (from 26.7 million to 21.7 million).[20] In March 2012, all major UK print newspapers announced a year-on-year decreases in headline circulation.[21] Public media and traditional broadcasting services such as the BBC have faced serious budgetary cuts, which have had a negative influence on their territorial and analytical coverage. Although readership of the print press in its traditional form has been steadily decreasing, online readership has been increasing, especially among younger generations. The available statistical data on circulations is provided by *OfCom* and includes the period immediately preceding this study. See Table 2.1. and 2.2.

Table 2.1. UK newspaper readership with their online versions, March 2013

Newspaper	Readership
The Sun	7,289,000
Daily Mail	6,232,000
Metro	3,621,000
Daily Mirror	3,149,000
The Guardian	2,316,000
Daily Telegraph	2,094,000

[18]Ibid.

[19]"Trust Polling: Political Monitor," February 2013, *IPSOS, MORI*, accessed on 18 September 2013, online at: http://www.ipsos-mori.com/Assets/Docs/Polls/Feb2013_Trust_Charts.pdf

[20]Moreover, the sector also faces challenges in terms of distribution, as it is getting harder to deliver newspapers to customers. The UK has very low rates of newspaper subscription compared to other countries (particularly European countries), which makes the British media sector very dependent on delivery services. See "The ownership of the news. Volume I: Report (HL Paper 122–I)", 27 June 2008, House of Lords, Select Committee on Communications - 1st Report of Session 2007–08, accessed on 15 September 2013, online at:
http://www.publications.parliament.uk/pa/ld200708/ldselect/ldcomuni/122/122i.pdf, p. 15.

[21]"Declining circulation of print newspapers occurs alongside shift in emphasis to online versions", March 2012, *OfCom*, accessed on 18 September 2013, online at: http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr12/internet-web/uk-4.58

Evening Standard (London only)	1,822,000
The Times	1,344,000
Daily Star	1,299,000
Daily Express	1,220,000
The Independent	902,000
Financial Times	408,000

Source: *OfCom* 2013, "Communications Market Report 2013".

Table 2.2. Online Reach of top 10 news sites in March 2013 (in %)
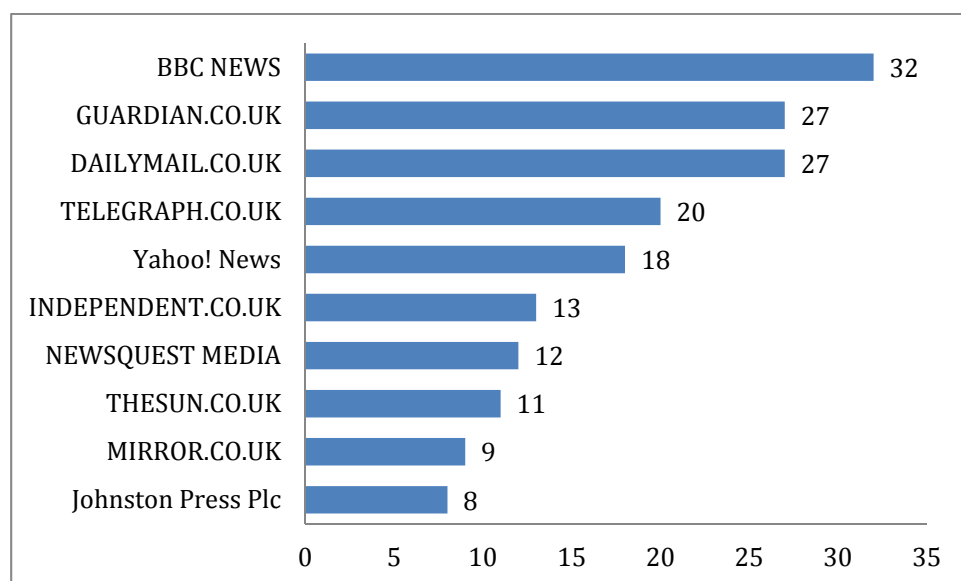
Source: *OfCom* 2013, "Communications Market Report 2013".

One of the strategies to lower costs is to rely more on multi-skilling and cut specialist correspondents, foreign bureaux, and investigative journalism, which has again only reinforced the trend of journalistic "dumbing down" (Temple 2008, 172). For many commentators, technology is to blame for forcing journalists to stress entertainment and abandon investigative and analytical journalism.[22] This trend, often referred to as "infotainment" and "tabloidization," has led to the rise of entertainment-focused papers in the UK at the cost of broadsheet circulation (McNair 2011, 60-63).[23] However, as Fenton (2009, 4) and also Temple (2008) noted, this trend is by no means new in the media industry and should not be framed simply around financial constraints imposed by freely available online resources. The positive aspects of new technology include the quantity, speed, and space allowed for news. Indeed, journalists and bloggers can produce an endless amount of

---

[22]"The ownership of the news. Volume I: Report (HL Paper 122–I)", 27 June 2008, House of Lords, Select Committee on Communications - 1st Report of Session 2007–08, accessed on 15 September 2013, online at:
http://www.publications.parliament.uk/pa/ld200708/ldselect/ldcomuni/122/122i.pdf, p. 29.
[23]"Ibid., p. 17.

news and update their reports within seconds. Moreover, the geographical reach of news produced in the UK is no longer dependent upon distribution contracts, but only by Internet accessibility and literacy.

After a short adaptation period, the press has managed to adjust its strategies to new trends by offering multimedia content and introducing Android and iPad versions of their titles. Hence despite the fall of the paper-based high-street press, e-newspapers reported as much as double the amount of visitors per day (in the case of *The Times*). In the UK, the first paper to introduce online content was *The Daily Telegraph* (Fenton 2010, 4), whose web content was also coded in this analysis. The Office of Communictions *(OfCom)*, the UK regulator of broadcast media, showed in 2013 that news is still a popular media product in the UK. 90% of all UK adults say they follow the news, whereby TV is the most important mode of news consumption (78% of UK adults use the television to learn news).[24] Traditional newspapers are used by 40% of UK adults to access news, radio by 35%, and the internet by 32%. As for newspaper readers, 24% read broadsheet newspapers and the same proportion read mid-market titles, while 37% read tabloids. As 80% of all British adults have access to the Internet at home and nearly a half of all British Internet users connect via their phones, it can be expected that the popularity of e-media will increase. The same survey also suggests that 54% of those who use the internet for news read e-news, while only a quarter read the relevant comments on blogs or social networks.[25]

The expansion of social media also brought about a change in journalism as a vocation. Any citizen can now become a journalist by covering and posting news via social networks or blogs (i.e. "User Generated Content"). This so-called civic journalism often merges the producer and the consumer into a "prosumer" (for more see Tumber 2001). The murky line between real and fake information is especially precarious on networks such as Twitter and Facebook. Twitter can be easily used for to spread invented messages. This tendency showed itself in April 2013 when the Associated Press's Twitter account was hacked and news about an alleged White House bombing caused havoc for some time.[26] But a second consequence is that even information that journalists are banned from making public, any private citizens has the means to spread globally. This is especially interesting in the case of the so-called superinjunctions in the UK. Superinjunctions "forbid the media from reporting certain information and even from reporting on the existence of the injunction itself" (Freedom House 2013). This has often led to the fact that the privileged elite are exempt from investigative journalism. The government has already asked social networks such as Google, Facebook, and Twitter to introduce monitoring systems

---

[24]"Communications Market Report 2013," 1 August 2013, *OfCom*, accessed on 18 September 2013, online at: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr13/2013_UK_CMR.pdf, summary.

[25]Ibid., summary.

[26]"Fake White House bomb report causes brief stock market panic." 23 April 2013, *CBC.ca*, accessed on 18 September 2013, online at:
http://www.cbc.ca/news/business/fake-white-house-bomb-report-causes-brief-stock-market-panic-1.1352024

which would catch any posts that violate superinjunction restrictions (Freedom House 2013).

Regulation and "the rules of the game" are important factors in the assessment of the media sector in the UK. Print media is only self-regulated. Each newspaper representative can choose to sit on the Press Complaints Commission, which assess individual cases of complaints. The Press Complaints Commission is an independent, non-governmental body, comprised of a number of serving editors, as well as a majority of independent, public members. It deals with complaints about published content and serves to hold newspapers to the Editors' Code of Practice.[27] The code lays out standards for ethics that balance and protect the rights of individuals as well as the freedom of the press. The Commission accepts complaints for free and strives to make itself easily accessible, lowering the barrier for individuals to make complaints. When a complaint is upheld, the adjudication is published in the offending newspaper or magazine. Most notably, after the 2011 phone-hacking scandal (often referred to as "hackgate") at the weekly *News of the World,* the government launched a public inquiry into the general regulatory framework of the British media market. One of the discussed topics was the excessive power of the media mogul Rupert Murdoch and his influence over British politics. The *News of the World* was owned by Rupert Murdoch, whose total newspaper holdings account for over 30% of newspaper sales in the UK.

The so-called "Leveson inquest" investigated and, in November 2012, produced a report containing recommendations about press regulation.[28] At the opening of the hearings in November 2011, Lord Justice Leveson summarized the aim of the inquiry as follows: *"The press provides an essential check on all aspects of public life. That is why any failure within the media affects all of us. At the heart of this inquiry, therefore, may be one simple question: who guards the guardians?"*[29] *According to the report published a year later, "media plurality is the cornerstone of a healthy democracy".*[30] That is why, among other things, the result of the inquiry was a series of recommendations for ownership regulation and the establishment of a new regulatory body, which would put an end to the simple self-regulation mechanisms. The creation of such a regulatory body is still under discussion, especially in terms of its statutory powers. As for now, the 2011 scandal uncovered an important flaw in the British media in terms of ownership. Unlike public media organizations, such as the BBC, which can afford to be independent, private media outlets and companies are often in hands of a few business monopolies with political interests.

---

[27]See "Editor's Code of Conduct," *Press Complaints Commission,* accessed on 18 September 2013, online at: http://www.pcc.org.uk/cop/practice.html

[28]The full report is accessible at "The Leveson Inquiry: The Report," 29 November 2012, *Leveson Inquiry: Culture, Practice and Ethics of the Press*, accessed on 15 September 2013, online at: http://www.levesoninquiry.org.uk/about/the-report/

[29]Included on the homepage of "The Leveson Inquiry" at *Leveson Inquiry: Culture, Practice and Ethics of the Press*, accessed on 15 September 2013, online at: http://www.levesoninquiry.org.uk/

[30]"Media Ownership: Summary," *The Leveson Report,* 29 Novemebr 2012, accessed on 15 September 2013, online at: http://www.levesoninquiry.org.uk/wp-content/uploads/2012/07/DCMS-submission_Narrative-on-media-ownership.pdf, p. 1.

The concentration of media ownership has been viewed as dangerous for democracy as fewer opinion-setters curbs the scope of public opinion and might limit the diversity of political debates (see Doyle 2002). To James Curran, this is nothing new as the British media has always been in the hands of a few powerful "press barons" throughout its history, such as Lord Northcliffe, Lord Beaverbrook and Lord Rothermere (Curran 2002). In his analysis, he noted that in 1937 four powerful men owned 50% of the UK media. As of 2013, the national newspaper industry in the UK is run by eight companies, whereby one has over 35% of the national newspaper market.[31] The regional and local press is owned by four publishers with almost 70% of the market. *Trinity Mirror* is the largest newspaper group in the UK, publishing 240 smaller, local and regional papers, in addition to its national papers. *News Corporation* is a multinational media company, which owns papers around the world, including *The Wall Street Journal* and *The New York Post* in the United States and many papers in Australia. *Independent Print Limited* is a company owned by Alexander Lebedev, a Russian oligarch. *The Daily Mail and General Trust plc* is a large British Media company. In addition to its national papers, it also has stakes in regional papers, radio, and television. *Northern and Shell* is owned by Richard Desmond, a British businessman, and publishes national papers and magazines, and also owns television channels. Radio news is dominated by the publicly funded BBC. National television news in the United Kingdom is produced by three companies: the BBC, ITN, and BSkyB.[32] In other words, the British media sector is highly centralized and owned by a small number of companies or individual businessmen, most notably the *News Corporation* of Rupert Murdoch.

Table 2.3. Newspapers and Owners

Owner	Papers
Telegraph Media Group	*The Daily Telegraph*, *The Sunday Telegraph*, *The Spectator* (weekly)
Pearson PLC	*The Financial Times*
News International (fully owned by News Corporation plc)	*The Time*, *The Sunday Times*, *The Sun*, *The Sun on Sunday*, *News of the World* (closed in 2012)
Scott Trust Limited	*The Guardian*, *The Observer*
Independent News & Media (Alexander Lebedev)	*The Independent*, *The Independent on Sunday*,
Daily Mail and General Trust plc	*Daily Mail*, *The Mail on Sunday*

---

[31]"The ownership of the news. Volume I: Report (HL Paper 122–I)," 27 June 2008, House of Lords, Select Committee on Communications - 1st Report of Session 2007–08, accessed on 15 September 2013, online at:
http://www.publications.parliament.uk/pa/ld200708/ldselect/ldcomuni/122/122i.pdf, p. 41.
[32]"The ownership of the news. Volume I: Report (HL Paper 122–I)," 27 June 2008, House of Lords, Select Committee on Communications - 1st Report of Session 2007–08, accessed on 15 September 2013, online at:
http://www.publications.parliament.uk/pa/ld200708/ldselect/ldcomuni/122/122i.pdf

Northern and Shell (Richard Desmond)	*Daily Express, Sunday Express, Daily Star, Daily Star Sunday*
Trinity Mirror	*Daily Mirror, Sunday Mirror, The People, Sunday Mail*

Source: "The ownership of the news", House of Lords, pp. 43-47.

After "Hackgate," proposals have been suggested to limit the ownership of any one person or company to 30%, with special permission needed from *OfCom* to gain control of more than 20%. Also of concern is the level of ownership of different types of media. *News Corporation*, owned by Murdoch, had its attempt to purchase full ownership of broadcaster *BSkyB* blocked in 2011.[33] The framework for UK commercial TV and local radio was anchored during the 1980s in the Broadcasting Acts of 1980 and 1981, and its revised version in 1990, which established the Independent Television Commission and the Radio Authority.[34] All of these acts, as well as subsequent 1996 and 2000 revisions, discussed relaxing the limit on ownership of the nominated news provider, originally set at 20%. In 2003, the limit was raised to 40% on TV and 55% on radio.[35] The 2003 the Communications Act set the so-called 20/20 rule on cross-media ownership, i.e. that "no one controlling more than 20% of the national newspaper market may hold more than a 20% stake in any Channel 3 service".[36] However, no definite decisions about limiting ownership in the wake of "Hackgate" had been made at the time of this analysis.

Save for the troublesome ownership disputes, the British media sector is quite free, with no serious limitations. However, security concerns always win over media freedoms. Though famous for its quality reporting, which was only reinforced by the abolishment of blasphemy and blasphemous libel in 2008, UK journalism is still limited by several restrictive legal provisions. Under the 1984 Police and Criminal Evidence Act, any media outlet is required to turn over its material to the police, as happened during the 2011 London riots, among other instances (Freedom House 2013).

Security thus has a direct impact on the nature of the published material. After the 2005 London bombing, where 52 people were killed and 700 injured, the government introduced a new Terrorism Act (2006), which criminalized speech inciting terrorist actions. A similar act in the same year outlawed any encouragements of racial and religious hatred and violence. This legislation is of course applicable to any type of online content and publicly accessible website. Since its adoption, several cases appeared whereby bloggers or owners of websites were charged with encouraging

---

[33]Justin Scholsberg, 8 March 2013, "Breaking the Silence," Media Blog LSE, accessed on 15 September 2013, online at: http://blogs.lse.ac.uk/mediapolicyproject/2013/03/08/breaking-the-silence-the-case-for-media-ownership-reform/

[34]"Media Ownership: Summary," *The Leveson Report*, 29 November 2012, accessed on 15 September 2013, online at: http://www.levesoninquiry.org.uk/wp-content/uploads/2012/07/DCMS-submission_Narrative-on-media-ownership.pdf, p. 4.

[35]See "The Media Ownership (Local Radio and Appointed News Provider) Order 2003 (SI 2003/3299)," *OfCom*, accessed on 15 September 2013, online at: http://stakehoders.ofcom.org.uk/market-data-research/other/media-ownership-research/rulesreview/

[36]Ibid.

racial or religious violence.[37]

Similarly, the number of cases where a person is accused of posting offensive comments on social networks has been growing. To some commentators, this imposes further restrictions on freedom of speech, since even online comments such as "UK soldiers should go to hell" or showing a burning poppy (the symbol of the UK remembrance day for World War I) have resulted in arrests and convictions.[38] These charges were raised in line with the 2003 Communications Act (Section 27), which prohibits any public and publicly accessible online statements which are "grossly offensive or of an indecent, obscene, or menacing character".[39]

With the expansion of social networks, even a seemingly harmless joke tweeted online can result in terrorist charges and have serious consequences since Twitter is a publicly accessible platform for anyone (unlike Facebook).

The British press, with its old tradition and renowned journalism, has a very particular position on the European media market. Fleet Street in London, the historical centre of British newspapers, symbolizes the long-standing tradition of serious and good journalism that hopes to empower people, strengthening democracy, and allow for a "collective view to evolve" (Temple 2008, 188). Although only one traditional generic broadsheet remains – *The Daily Telegraph* – the British press still offers a variety of respectable papers covering political issues.

Moreover, unlike in the past, the mainstream media now cuts across all political allegiances and partisanship, although newspapers still align themselves with specific political views. The most recent technological changes have slowly been moving the readership onto electronic platforms while decreasing the number of traditional press readers. The advance of online media has also spurred discussions about changes in the field of press regulation and ownership transparency since the media have historically functioned on a self-regulating basis. The British press, just like any other in the 21st century, is thus currently undergoing some major structural and editorial changes to reflect the challenges of the changing nature of the public sphere. This is also the reason why this paper discusses topics related to these modern technological changes while using online platforms.

3. Methodology

---

[37]The most famous one is the case of a 23-year old blogger, Bilal Zaheer Ahmad, who was sentenced to 12 years for calling for the murder of MPs supporting the war on Iraq. See "Blogger who encouraged murder of MPs jailed", *BBC*, 29 July 2009, accessed on 28 August 2013, online at: http://www.bbc.co.uk/news/world-14344199.

[38]See Jill Lawless, 15 November 2012, "In UK, Twitter, Facebook rants land some in jail", *Bigstory.ap,* accessed on 28 August 2013, online at: http://bigstory.ap.org/article/uk-twitter-facebook-rants-land-some-jail.

[39]See "Communications Offenses", *The Crown Prosecution Service*, accessed on 28 August 2013, online at:http://www.cps.gov.uk/legal/a_to_c/communications_offences/

The selected methodological approaches for this analysis were chosen within the scope of the SECONOMICS project and are uniform for all case studies. The principle method is qualitative textual content analysis of a purposefully selected sample of articles from *The Guardian* and *The Daily Telegraph*. For comparative purposes, only articles published between 1 January 2010 and 31 April 2013 were selected and coded by a set coded scheme (Guasti 2013). The SECONOMICS project identified three topics of analysis which branch out into different fields and disciplines. The topic of CCTV and surveillance is closely related to the transport case study of the SECONOMICS project, but also political science in terms of its relevance for power relations and regulation. Similarly, 3D body scanners are examined in security studies and the field of public policy due to their relevance to air transport security. The topic of Stuxnet has implications for the field of state intelligence and international relations, and in the SECONOMICS comparative media research it plays the role of a proxy for studying critical infrastructure vis-à-vis printed media. Combining these three topics through the prism of media content analysis, we aim to present and analyse the primary trade-offs of security management and how these are portrayed in the media and by various stakeholders.

This approach allows us to meaningfully study the range of topics, but also discourses which surround the three studied themes. Media frames topics and transmits messages about events, which are accepted or critically evaluated by readers. Studying the content of a large number of newspaper articles would be impossible without research software such as *Atlas.ti7*, which we use to code a sample of carefully selected articles in two newspapers per country. The articles analysed were representative of the overall coverage in the given country over time, per topic and per newspaper. Codes were assigned to any statements about CCTV, 3D body scanners, or Stuxnet respectively. These codes identified related topics, actors, argumentative strategies, justifications, and lines of argumentation (see Guasti 2013).

This report is based on a selection of articles from two national newspapers from the United Kingdom, one left-leaning and one right-leaning. Due to their availability online and the ability to search through their archives, we have focused on their electronic versions. The left-leaning paper is the respected daily broadsheet, *The Guardian,* and the right-leaning paper is *The Daily Telegraph.* In order to select which newspapers to use, circulation data about national newspapers was gathered and evaluated. The highest-circulated left- and right-leaning quality papers were selected.

The Guardian was founded in 1821 under the title *The Manchester Guardian,* but shortened its name in 1959. Alan Rusbridger is its current editor in chief. *The Guardian* is part of *The Guardian Media Group* and is currently owned by Scott Trust Limited, a limited company. However, the paper is also supported by a number of external investments. The management of the paper is unlike any other in the UK, as it is answerable only to the Trust and has no shareholders or proprietor. There is a public ombudsman, who assess complaints and comments from readers on the paper's content. Regarding its readership, *The Guardian* is a daily of the

young and liberal readers, who are also largely Labour voters (Anderson, Williams, and Ogola 2013). Given decreasing print edition sales, the management of the paper has invested heavily in its online version, which has over 3,4 million daily visits (Ibid, 106).

The Daily Telegraph is regarded as the "Conservative Party House Paper" and is predominantly a paper of the British middle class (Anderson, Williams, and Ogola 2013, 105). It was founded in 1855 as *The Daily Telegraph and Courier*. Tony Gallagher is its current editor in chief. *The Daily Telegraph* was a pioneer in digitalized online newspapers. In 1994, it launched the first multi-platform digital newsroom in the UK and was the first paper in the UK to introduce a paywall for its content in 2011. Since 2004, it has been in the private ownership of David and Frederick Barclay and it is currently the only quality paper to turn a profit.

Once the newspapers were selected, articles on each of the three topics—CCTV, Stuxnet, and 3D body scanners—were then downloaded from the newspapers' websites. The articles were located by using the search functions available on the websites. The phrases used to search were simply the name of the topic: "CCTV" for CCTV, "stuxnet" for Stuxnet, and "body scanner" for body scanners. From the search results, the articles in the selected time range of the analysis (January 2010 - April 2013) actually relevant to the topics were downloaded. Some articles only mentioned the search terms in passing and were not actually relevant to the topic. This occurred most often for the CCTV topic, where a large number of articles mentioned CCTV in passing, as a reference to how a crime was observed, for example, rather than discussing it as a topic.

Table 3.1. Number of Articles by Topic and Year

Newspaper	Topic	2010	2011	2012	2013	Total
The Guardian	Body Scanner	34	8	5	1	48
	Stuxnet	7	7	5	2	21
	CCTV	11	6	8	0	25
The Daily Telegraph	Body Scanner	10	6	1	0	17
	Stuxnet	5	18	14	1	38
	CCTV	6	6	3	3	18
	Total	73	51	36	7	167

Source: SECONOMICS UK sample

In total, 167 articles were selected and downloaded from both websites on all the topics (see Table 3.1). The largest number of articles came from 2010, a year during which *The Guardian* published 34 articles about body scanners. This is significantly more than any other year or topic. This was due to the fact that at that point the topic of 3D body scanners was being widely discussed by the public and media. The number of articles in 2013 is much lower than in other years, as it was near the beginning of this year

when the articles were collected. The number of articles for each topic and year was scaled so that the total number of articles was close to 40, the target number of articles for each of the country reports. The proportion of articles for each year for each topic in the adjusted numbers was kept close to the original ratio. This resulted in a total of 43 articles (see Table 3.2). Using the adjusted numbers, articles were then selected from those downloaded. For example, seven articles were selected on the body scanner topic from *The Guardian* for 2010. The articles were chosen to reflect the varieties of opinion and writing style present in the original sample as much as possible. In other words, we used a purposeful sampling method to choose articles for coding, as random sampling would not yield the required diversity of themes and opinions.

Table 3.2. Adjusted Number of Articles by Topic and Year

Newspaper	Topic	2010	2011	2012	2013	Total
The Guardian	Body Scanner	7	2	1	0	10
	Stuxnet	2	2	1	1	6
	CCTV	3	2	2	0	7
The Daily Telegraph	Body Scanner	3	2	1	0	6
	Stuxnet	1	4	3	0	8
	CCTV	2	2	1	1	6
	Total	18	14	9	2	43

Source: SECONOMICS UK sample

4. Analysis

4.1 Descriptive Analysis

4.1.1. 3D Body Scanners

The main actors in the debate about body scanners are journalists, government entities and politicians, such as departments and ministers, and civil liberties advocacy groups. There are also individual passengers, transport companies, and health experts.

Figure 4.1. Actors and argumentative strategies
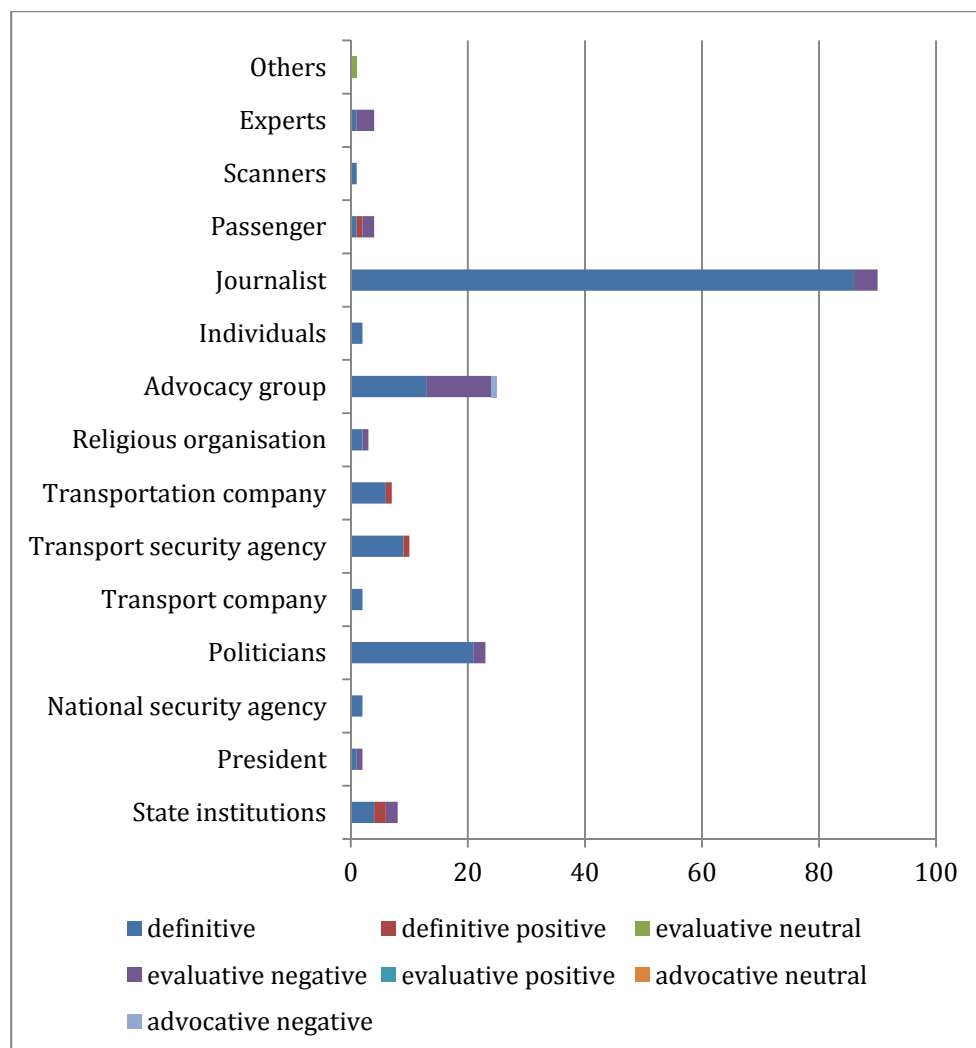
Source: Seconomics UK sample

The civil liberties advocacy groups most often present in the analysis include: 1) Action for the Rights of Children, a UK non-profit group working for the human rights of children; 2) Liberty, a UK-based group that defends civil liberties; 3) Privacy International, a UK-based group focused on protecting privacy rights around the world; 4) Electronic Privacy Information Center, an American group for the protection of privacy and civil liberties;

5) The Equality and Human Rights Commission, a public body in Great Britain which promotes and protects human rights; and 6) Big Brother Watch, an UK civil liberties and freedoms group.

Government actors most often present in the analysed articles include: 1) Gordon Brown; 2) Department for Transport; 3) Barack Obama; 4) Transport Minister; 5) Counter-terrorism Minister; 6) The Transportation Security Administration.

Over the course of the studied time period, there were three main issues discussed in the articles about body scanners. The first is the legality of the introduction of the new types of scanners in regards to privacy rights. The second is whether the images produced by the scanners violate child pornography laws. The third is possible health issues related to the scanners.

The first issue is the most dominant and is present from 2010 through 2012. The second is also present in several articles at the beginning of 2010, but only remains a topic for a short time period. The final issue, the possible health dangers of scanners, is introduced into the debate in a small number of articles in 2011 and after.

The relationship between two of the main groups of actors, government institutions and advocacy groups, is readily apparent. The government is very much in favour of the introduction of body scanners, and the civil liberties groups oppose them on the basis of privacy and legality. A good example of the government position was presented in *The Guardian:*

> Speaking on BBC One's Andrew Marr programme, Gordon Brown pre-empted the findings of his own review by saying future passengers must expect to be scanned by the controversial scanners. (Stratton 2010)

The reaction of one civil liberties group, also in *The Guardian,* points towards apprehensions that the body scanners will be used without respect for passengers' religious views and that it might target some racial groups:

> But Shami Chakrabart, of Liberty, had concerns over the "instant" introduction of scanners: "Where are the government assurances that electronic strip-searching is to be used in a lawful and proportionate and sensitive manner based on rational criteria rather than racial religious bias?" she said. (Alan 2010)

There is a dialogue between the two sides of the debate, as the government responds to the questions about privacy. From *The Daily Telegraph*:

> A Department for Transport spokesman said: "We understand the concerns expressed about privacy in relation to the deployment of body scanners, which is why we have drawn up a code of practice for their use. This will ensure operators are separated from the passengers being screened, and these anonymous images are

destroyed after scanning is complete. (2010 Airport body scan images)

The argumentative strategies used in the articles are indicative of the interaction between the government, trying to introduce the new scanners, and its opponents, the civil liberties groups. Politicians made 21 definitive statements in the articles, and just 2 evaluative statements. In contrast, advocacy groups made 12 definitive statements, and 11 evaluative statements—all of which were negative. The politicians set out their policy, as in *The Guardian:*

The transport minister Paul Clark told MPs a random selection of passengers would go through the new scanners at UK airports. (Travis and Milmo 2010)

This was then subject to criticism by the advocacy groups. The negative evaluations were not limited to just the civil liberties groups. Experts had three negative evaluative statements, and passengers had two. The experts commented on the effectiveness of the new machines:

The prime minister's evident decision to support the installation of new £100,000 body scanners will be criticised since many industry insiders believe the machines are flawed. (Stratton 2010)

Journalists had the highest number of definitive statements, 86, of any of the actors in the coding scheme, which is not surprising as these statements are mostly informative. The four evaluative statements from journalists were in editorial articles, such as this one from *The Guardian*:

When a whole-body scanner in an airport falls foul of child pornography laws, my immediate thought is that those laws are wrong. (Williams 2010)

The justification of privacy is the most used from the coding scheme, with 12 statements. This is followed by legality and freedom/liberty with four statements each. Below this are health, dignity, and efficiency, with three each. This makes sense, as a greater number of articles were concerned about privacy than health. The privacy justifications are present throughout the entire time range, and the health justifications occur only with the articles concerned with the impact of x-rays, which start from 2011.

Table 4.2. Number of occurrences of topics

Body scanner	80
Privacy	65
Security, rules and regulations	59
Terrorism	26
Security, general	20
Health issues	17

Freedom	12
Increased number of body scanners	6

Source: SECONOMICS UK sample

4.1.2. CCTV

In the articles on CCTV, the actors with the most statements—besides journalists—are politicians and police, followed by city councils and advocacy groups.

Figure 4.3. Actors and argumentative strategies
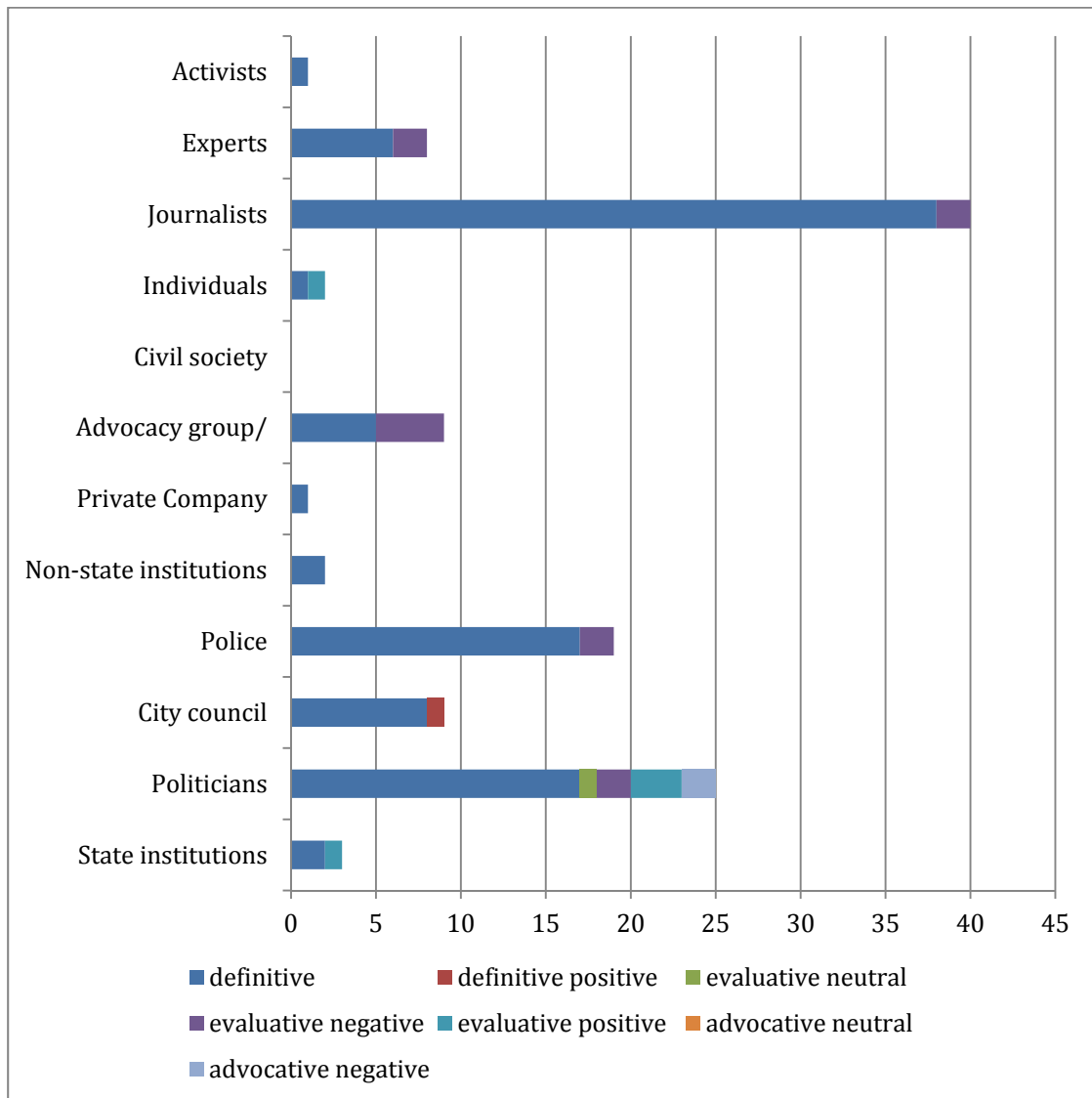
Source: SECONOMICS UK sample

The figure above can be summarized as follows: there are several different topics of discussion in the CCTV articles. First is the inappropriate use of CCTV. Then there are several articles that discuss the fact that Britain is becoming a surveillance society. Other articles discuss the potential

dangers of new monitoring and camera technology. Rules and regulations surrounding the use of CCTV are also a topic of discussion.

The topic of inappropriate use of CCTV includes articles that discuss the installation of CCTV cameras for counter-terrorism purposes in a Muslim neighbourhood in Birmingham, but under the guise of crime prevention, as well as an article about the use of CCTV for monitoring the behaviour of students in schools, and an article about the installation of CCTV in taxis.

The actors involved in this topic are city councils, with 10 statements, the police, with 9, journalists, with 8, politicians, with 7, and advocacy groups, state institutions, and non-state institutions with 2 each.

In the Birmingham case, the local politicians attacked the scheme, about which they had been misled. *The Guardian* reported that:

> Tanveer Choudhry, a [Liberal Democratic] councillor for Springfield ward, said they should be "taken down immediately" rather than mothballed. "What the community wants to see is the cameras removed and a full investigation into how they were put up in the first place without consultation…
>
> Parliament has been asked to denounce Project Champion as a "grave infringement of civil liberties" … by the Labour MP for Birmingham's Hall Green constituency, Roger Godsiff (Lewis 2010).

The police and council initially defended the installation of the cameras:

> Although the counter-terrorism unit was responsible for identifying and securing central government funds… the camera sites were chosen on the basis of general crime data – not just counter-terrorism intelligence. Day-to-day management of the network was always intended to become the responsibility of local police. (Lewis 2010a)

But they eventually decided to remove the cameras:

> We can fight crime and the threat posed by terrorism far more effectively by working hand in hand with local people, rather than alienating them through a technological solution which does not have broad community support. (Lewis 2010b)

The civil liberties group Liberty also joined in the debate:

> The civil rights organisation Liberty wrote to the force last week, threatening to commence judicial review proceedings at the high court unless the force agreed within 14 days to "dismantle the full surveillance infrastructure". (Lewis 2010b)

In contrast to this case, the article on the use of CCTV in schools doesn't contain evaluative statements reacting to the use of CCTV. Instead, the article in *The Daily Telegraph* uses only definitive statements to report a

study:

> The latest study, which features contributions from a series of academics, said: "The use of CCTV has migrated from perimeter security and access control to monitoring pupil behaviour in public areas such as in corridors and playgrounds, and to more private realms such as changing rooms and toilets." (Paton 2010)

It is interesting that there is no commentary from politicians or civil rights groups about the privacy issues in this case, merely a statement saying "cameras should only be used to monitor behaviour in exceptional circumstances."

The last case, the installation of CCTV cameras in taxis, does include strong responses from civil rights groups. The justification of crime prevention is used by the local council in defence of the scheme in the *Telegraph* article:

> The risk of intrusion into private conversations has to be balanced against the interests of public safety, both of passengers and drivers. (2011 "Recording taxi conversations")

The response is a strong, negative evaluative statement coded with "right to privacy" and "freedom/liberty" as justifications:

> Nick Pickles, the [Big Brother Watch] campaign group's director, said: "This is a staggering invasion of privacy, being done with no evidence, no consultation, and a total disregard for civil liberties." (ibid.)

The next topic is the increase in CCTV cameras in the UK and its movement towards becoming a surveillance society. The actors in these two articles are experts, with 7 statements, journalists, with 4, politicians, with 3, police, with 2, and advocacy groups and state institutions, with 1 each. There are 12 definitive statements, 2 evaluative, and 3 advocative.

The first article, from *The Guardian*, is about a report by the Surveillance Studies Network. It uses definitive and evaluative statements to describe the contents of the report:

> There continues to be a major problem with CCTV systems and automatic number plate recognition [APNR] cameras that read thousands of car number plates an hour and identify their owners through a live DVLA link. The authors say this undermines transparency and accountability. (Travis 2010)

It has an advocative statement describing the information commissioner's response:

> Information commissioner Christopher Graham is pressing ministers for new privacy safeguards in the wake of a report that suggests moves towards a surveillance society are expanding and intensifying.

(Travis 2010)

The next article, also from *The Guardian*, describes a study to estimate the number of CCTV cameras present in the UK by physically counting the cameras in one area and then extrapolating to the rest of the country. The results estimate about 1.85 million cameras in the UK, or one camera for every 32 people. The article contains only definitive statements, the majority of which are from the police, who commissioned the report:

> Cheshire's deputy chief constable, Graeme Gerrard, said the data undermined more sensational estimates, such as the widely-repeated but dubious claim that the average Briton passes under 300 cameras a day. (Lewis 2011)

The article contains a response to the study, in the form of a definitive statement, from a civil rights group:

> Isabella Sankey, director of policy at the campaign group Liberty, echoed the wider concern. "Who cares if there is one camera or 10 on their street if that one camera is pointing into your living room. Concerns about CCTV are not a simple numbers game; what's required is proper legal regulation and proportionate use." (Lewis 2011)

Another topic is the use of newer, more advanced CCTV technology. There are two articles from *The Guardian* on this topic. The actors in these articles are journalists, with 8 statements, experts, with 2, and politicians, private companies, and individuals, with 1 statement each. The statements are mostly definitive (10), with 2 evaluative statements and 1 advocative.

The first article describes a new surveillance system called Trapwire, which is capable of recognising people on CCTV camera and analysing their behaviour to identify possible terrorist threats. The article uses purely definitive statements from the company that designed the system as well as other experts to describe the technology:

> Stratfor describes Trapwire as "a unique, predictive software system designed to detect patterns of pre-attack surveillance and logistical planning" (Arthur 2012)

The next article is an editorial about the threats to privacy posed by new technology. As it is an editorial, it has a number of statements by the journalist, using definitive, evaluative, and advocative argumentative strategies. Advances in software mean that cameras that previously once just recorded could soon be used to identify and track:

> All the cameras currently operating "for your security" can be updated and converted to recognise faces. Wherever you go, someone will be logging your movements – whether it is the police or the big supermarket chains that are anxious to monitor the behaviour of customers in their stores. But the vital fact to remember is that all private CCTV cameras may be accessed by the authorities and are

therefore, in effect, part of the state's surveillance system. (Porter 2012)

The author concludes the article by advocating for a privacy law:

> We need a privacy law … a bill in parliament [SIC] that asserts our right to guard our privacy against the state, corporations and the malevolence of future governments. (Porter 2012)

The final topic in the articles about CCTV is the rules and regulations that govern CCTV use. A number of the articles discussed previously have mentioned the need for new or improved regulations for CCTV, such as Porter (2012), Lewis (2011), and Travis (2010). There are two articles not yet mentioned that are about this topic, both from the *Daily Telegraph*. The actors in these two articles are journalists (13 statements), politicians (7), advocacy groups (4), and police (2 statements). There are 24 definitive statements, and just 1 evaluative and 1 advocative statement.

The first article is about the introduction of regulations for traffic (ANPR) cameras. All but one of the statements is definitive, and the journalist is almost the only actor in the story. The regulations are designed to increase transparency and help control the data generated by the system:

> However, the Home Office will now introduce new regulations forcing police to be more transparent with the public about locations and numbers of cameras, as well as clarifying and limiting who has access to the database. (Watt 2010)

The only non-definitive statement in the article is a negative evaluative statement from a civil rights group:

> Dylan Sharpe, the campaign director of Big Brother Watch, said: "APNR cameras are an unnecessary and indiscriminate invasion of privacy." (Watt 2010)

The other article is about the introduction of the Protection of Freedoms Bill, part of which allows the public to challenge their local councils in court if cameras are being used inappropriately. Most of the statements are definitive, and the article has statements favourable to the bill from politicians and advocacy groups:

> Nick Clegg, the Deputy Prime Minister, said the bill is an unprecedented move to restore personal liberties and will put "the brakes on the surveillance state".

> David Green, director of the think-tank Civitas, said it was the largest redress of civil liberties since the 1689 Bill of *Rights.*

Table 4.4. Number of occurrences by topics

Cameras, CCTV	70
Security related rules and regulations	37
Surveillance	26
Privacy	15
Counter terrorist system	11
Surveillance increase	10
Freedom	7
Crime prevention	7
Terrorism	6
Crime solution	4
Crime detection	3
Personal data protection	3
Personal freedom	3
Purchase/installation of CCTV cameras	2
Public domain monitoring	2
Protest	2
Costs	2
Security general	2
Power	1
Freedom of movement	1

Source: SECONOMICS UK sample

4.1.3. Stuxnet

In the third topic, the Stuxnet computer virus, there are two categories of actors that have many more statements than others: journalists and experts. This reflects the topic and the style of writing around it. It is highly technical, with a lot of commentary by computer security researchers.

Figure 4.5. Actors and argumentative strategies
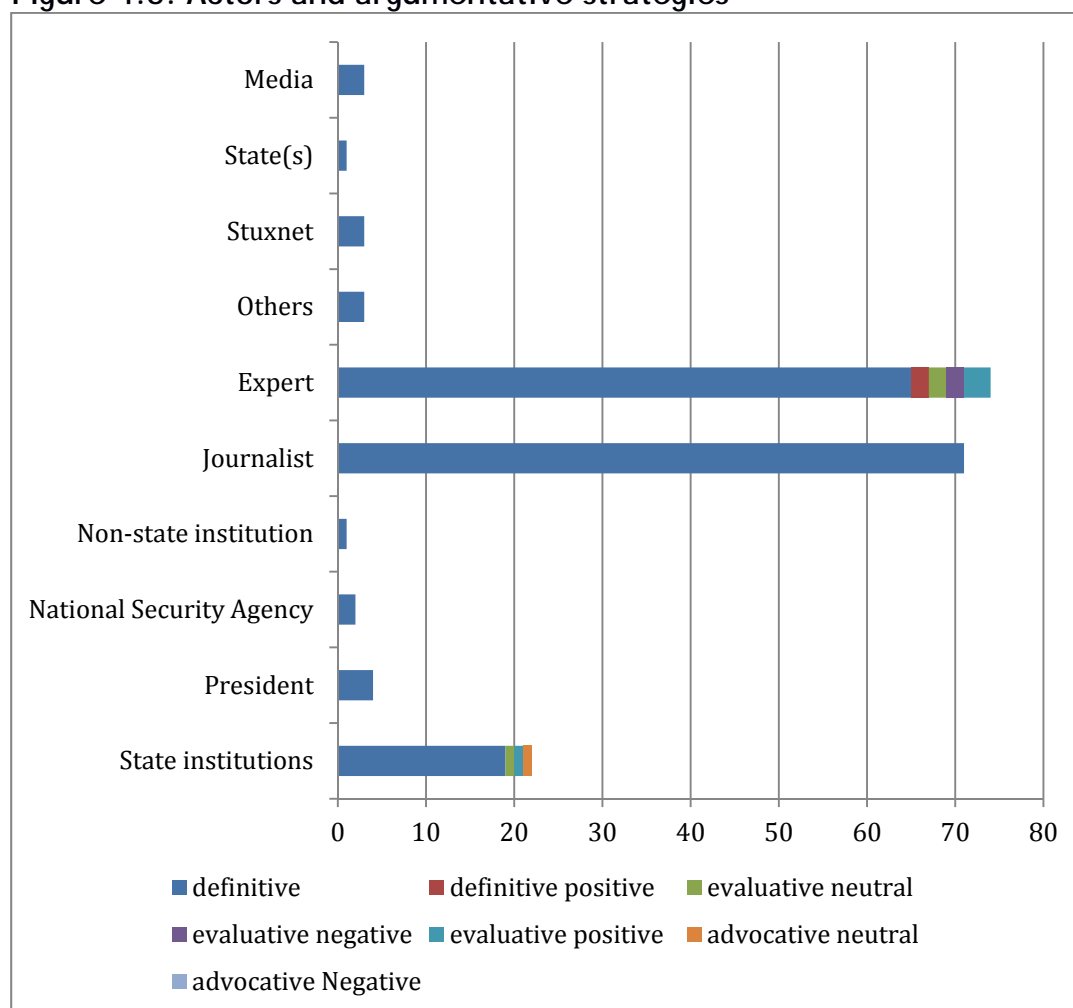
Source: SECONOMICS UK sample

The articles on Stuxnet focus on a few different topics. In the earlier articles, the purpose of Stuxnet is a main topic. The question of the identity of the worm's creators is also present in a large number of the documents, as well as its relation to another sophisticated virus, Flame. And finally, the topic of cyber-warfare and the UK's preparedness and capabilities becomes a topic in later articles.

In the earliest articles, relatively little is known about the creator or target of the worm:

> David Emm, a senior security researcher at Kaspersky Lab, told the Guardian: "We think that Stuxnet's sophistication, purpose, and the intelligence behind it suggest the involvement of a state." (Halliday 2010)

> "The fact that we see so many more infections in Iran than anywhere else in the world makes us think this threat was targeted at Iran and that there was something in Iran that was of very, very high value to whomever wrote it," Liam O'Murchu, an expert at Symantec, told the

BBC. (Beaumont 2010)

Subsequent articles have more information about the target of the attack, the Iranian nuclear enrichment program:

> Now new research by cyber security firm Symantec shows definitively that Stuxnet was built to target uranium enrichment equipment used to fuel Tehran's controversial nuclear programme. (Halliday 2010)

It became suspected that the US and Israel were behind the development of Stuxnet:

> "It was most likely developed by a Western power, and they most likely provided it to a secondary power which completed the effort," Tom Parker, a security research, told the Telegraph, naming the US and Israel as the most likely pairing. (Williams 2011)

This suspicion was eventually confirmed in 2012:

> The disclosures about Obama's role in the cyberwar against Iran appear to show beyond doubt that the US, with the help of Israel, was behind the Stuxnet virus, which sent some of Iran's centrifuge machines – used to enrich uranium – spinning out of control. (Beaumont and Hopkins 2012)

The discovery of Stuxnet and its level of sophistication started a discussion about the future of cyber-attacks and cyber warfare:

> The strategic defence and security review said: "Over the last decade the threat to national security and prosperity from cyber-attacks has increased exponentially… We will also work to develop, test, and validate the use of cyber capabilities as a potentially more effective and affordable way of achieving our national security objectives." (Hopkins 2011)

There is concern that the UK might be falling behind in its ability to defend itself in terms of more sophisticated cyber-attacks:

> What concerns the Government is the remaining 20 per cent – those products of more sophisticated criminal minds, intelligence services and military establishments that are specifically designed to breach the defences either of companies or of the so-called Critical National Infrastructure (CNI). And this is where we might be falling behind. (Glenny 2012)

Attacks of the complexity and sophistication of Stuxnet are going to become more regular:

> Professor Peter Sommer, a computer forensics expert at the London School of Economics and Political Science, said the Stuxnet attack's complexity in both the digital and physical realms was very

impressive. However, he added that the virus itself heralds only an evolutionary stage in the cyber security threats that nations will face in the future.

> "We should see this as another type of tool in statecraft," Professor Sommer, who advises the OECD on cyber security, said. (Williams, 2011)

If attacks of this level are going to become common then it is imperative that the UK respond to the threat. Indeed, one of the only advocative statements in all the articles about Stuxnet urges that Britain increase its spending and offensive cyber capabilities:

> Not only do we need to spend more, the [Commons select committee on intelligence and security] implies for the first time that Britain should ramp up its "active" defence strategy to keep pace with the proliferation of cyber-attacks that rain down on our institutions, companies and citizens every day. (Glenny, 2012)

Table 4.6. Topics, number of occurrences

Stuxnet	64
Attack on Iran	45
Iranian uranium enrichment program	44
USA	27
Israel	26
Development of Stuxnet by a state	25
Security general	24
Development of Stuxnet	20
Cyber war	17
Attack	16
Flame	14
Security related rules and regulations	5
Olympic games	4
Terrorism	3
Deployment/attack using Stuxnet	3
State accused of attack	3
Attack on other state	2
Government-led antiterrorism campaign	1

Source: SECONOMICS UK sample

4.2 Analysis of General Tendencies

In identify general tendencies in reporting on security issues in the UK between January 2010 and April 2013, we will now compare the three above

analysed debates. In the British press, each topic represents different patterns – various sets of actors were involved in each debate, different types of interaction among these actors took place and, most importantly, the intensity of the debates varied. Overall, journalists played the most important role in all three debates – in the body scanner debate they led the debate by a wide margin, with advocacy groups and politicians placing a distant second. In the CCTV debate, a much smaller gap existed between journalists, who led, and politicians and police. The exception to this pattern is the Stuxnet debate, where experts replaced journalists as the dominant actor. However, journalists were still the second most common actor, followed by the state institutions in a distant third.

The main themes of the debates also varied. The body scanner articles' main topics were the legality of introducing such a security measure. This was mainly debated in terms of privacy rights, but interestingly the question was also raised about whether or not the scanners violate child pornography laws. Last but not least, health issues related to the scanners were also raised. Opinions about the introduction of body scanners varied among the actors involved. Politicians pushed for the introduction of the new scanners, which ought to provide additional security and reduce terrorist threats. On the other hand, civil rights advocacy groups rejected the body scanners, arguing that the scanners violated privacy laws. There was a dynamic and intense debate between these two kinds of actors on the subject of privacy and the breach of human rights in terms of "leaving citizens alone" as discussed in the background section.

In articles discussing CCTV, the main topics were several instances of the inappropriate use of CCTV, Britain's movement towards becoming a surveillance society, the dangers new technology poses to privacy, and changing rules and regulations about the use of CCTV. The CCTV debate was significantly more substantive than the body scanner debate. The most important issue was the misleading of the public in the case where cameras were installed for anti-terrorism purposes, but said to be for crime-prevention. This fact was discovered by *The Guardian*, which continuously addresses this issue. Aside of journalists and politicians, civil rights groups were also involved in this debate. Another exchange took place between journalists, civil rights groups, and city councils in debate regarding the installation of CCTV in taxis. Aside of these two themes, the rest of the CCTV articles involve significantly less debate and less disagreement. The most agreement is found in the articles about Britain becoming a surveillance state and the dangers of newer technology. The actors here are the government and civil rights groups, who both seem to be aware of the dangers of excessive surveillance and move to enact new legislation to regulate its use.

In the Stuxnet articles, the main topics were the explanations of the purpose of the virus, the attempts to uncover identity of its creators, and the implications of this type of attack on defence and cyber warfare. The Stuxnet articles are about a highly technical subject, and the actors reflect that. There are a large number of statements by experts explaining details of the virus's operation. The expert and technical character of this debate

is further characterized by the almost full absence of any debate. The articles were mostly just reporting new information about Stuxnet, and a large part of most articles was devoted to explaining the technical details of its application.

The use of argumentative strategies in the three debates also differs. Evaluative statements dominate the body scanner debate, reflecting the criticism of this security measure by civil rights groups. Advocative statements dominate the CCTV debate, as there was adovcacy from rights organizations, as well as government agencies and individuals for increased safeguards for privacy. The Stuxnet debate was dominated by definitive statements – as explained above, due to the expert and technical character of the debate. However, the Stuxnet debate also included some advocative statements, which called for the use of cyber-attacks instead of conventional attacks, and also argued for an increase in spending on cyber defences.

Overall, most definitive statements were by journalists, with the exception of Stuxnet articles, where the greatest number was by experts. The lack of debate in the Stuxnet articles explains why definitive statements have the highest percentage, 91%, of all three topics, compared to 1% and 82% of statements for CCTV and body scanners, respectively. The intensity of debate correlates to the use of evaluative statements.

In terms of the direction of the debate, the topic of privacy in the body scanner and CCTV debates was most often framed negatively by civil rights groups, criticising policy that threatens privacy and individual freedoms. The strongest debate, about body scanners, has the highest level of negative evaluative statements, and Stuxnet, with the least debate, has the lowest.

Table 4.7. Number of instances of topics

	Body scanner	CCTV	Stuxnet
Security related rules and regulations	59	37	5
Privacy	65	15	0
Security general	20	2	24
Terrorism	26	6	3

Source: SECONOMICS UK sample

The articles on body scanners and CCTV share a common focus on privacy and security, and security rules and regulations, and to a lesser degree on terrorism. The focal point of the body scanner and CCTV debate is security and privacy vis-à-vis the individual. In contrast, the Stuxnet articles security and security rules and regulations, refer to national security—critical national infrastructure, and (international) laws about cyber warfare (and lack thereof). Cyber terrorism is here seen as a specific form of

terrorism.

Table 4.8. Major actors and argumentative strategies

		Definitive	Evaluative	Advocative
Journalist	Body scanner	86	4	
	CCTV	38	2	
Expert	Stuxnet	71		
	Body scanner	1	3	
	CCTV	6	2	
State Institution	Stuxnet	65	6	3
	Body scanner	4	4	
Politician	CCTV	2		1
	Stuxnet	19	1	2
	Body scanner	21	2	
	CCTV	17	3	5
Police	Stuxnet			
	Body scanner			
	CCTV	17	2	
Advocacy Group	Stuxnet			
	Body scanner	13	11	1
	CCTV	5	4	
	Stuxnet			

Source: SECONOMICS UK sample

Table 4.9. Argumentative strategies per topic

	Definitive	Evaluative	Advocative
Body Scanner	149 (82%)	31 (17%)	1 (1%)
CCTV	95 (81%)	16 (13%)	7 (5%)
Stuxnet	174 (94%)	6 (3%)	5 (3%)

Source: SECONOMICS UK sample

Conclusions

The three security debates in the British press show interesting similarities and differences. The most important difference is the object of security. In the case of the CCTV and body scanner debates, the individual is at the heart of the debate. Modern individuals benefit from security measures meant to decrease the threat of terrorism, but do so at the cost of their privacy and civil rights. In the Stuxnet debate, on the other hand, the object of security is the state and concerns focus on national security and critical infrastructure.

In the British debate we see strong awareness of the trade-offs between privacy and security. Civil rights groups object to the unregulated introduction of body scanners, insisting on privacy, but also raising issues such as human dignity, respect for religious freedom and diversity. This clearly demonstrates that new technological and security measures can also raise new issues and that acceptance of such measures depends on cultural factors, but also on whether the public believes that new measures will be used in a regulated way.

To a lesser degree this dynamic is also present in the CCTV debate. Increasingly, the use of CCTV as a general security measure is questioned and a clear delineation between crime prevention and anti-terrorism is required. When public acceptance of CCTV in crime prevention was used as a smoke screen for anti-terrorism, there was a negative backlash against the measure. Civil rights organisations fight to regulate the use of CCTV, as well as other new and emerging technological surveillance threats to privacy and civil liberties. And so in the body scanner debate, where the national government is pressing for the new technology, and in CCTV debates, where the police and local councils are implementing measures that threaten privacy, these forces face increasing opposition.

The Stuxnet discussion, with its absence of debate, also raises important questions, but on other, more abstract levels. First, it shifts the debate from the domestic to the international arena. But it also moves from the relationship between citizens and the state, as regulated by domestic law, to the relationships between states themselves, as regulated by international law. And finally it shifts the debate from conventional warfare with physical objects, to cyber warfare with digital weapons. The Stuxnet debate also reveals one particularly dangerous tendency – namely that if an issue is more technically complex, then it will generate less debate. However, as we demonstrate here, complex matters can prove quite influential on important issues, which, while not concerning citizens directly, have far reaching implications for critical national infrastructure and the ways in which modern states interact with each other in the absence of international law and behind the smoke screen of anti-terrorism.

References

Anderson, Peter J., Michael Williams, and George Ogola. 2013. *The Future of Quality News Journalism: A Cross-Continental Analysis*. Routledge.

Barnard-Wills, David. 2011. "UK News Media Discourses of Surveillance." *The Sociological Quarterly* 52 (4): 548–567.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. Vol. 17. Sage.

Beckman, James. 2013. *Comparative Legal Approaches to Homeland Security and Anti-terrorism*. Ashgate Publishing.

Breau, Susan, Stephen Livingstone, and Rory O'Connell. 2002. *Anti-Terrorism Law and Human Rights in the United Kingdom Post September 11*. Queens University Belfast: British Council. http://www.britishcouncil.org/china-society-publications-911.pdf.

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

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. 2011. *Cyber Security and the UK's Critical National Infrastructure*. Chatham House. https://www.baesystemsdetica.com/uploads/CHA732_Cyber_report.pdf.

Curran, James. 2002. *Media and Power*. Communication and Society. Routledge.

Denney, David. 2005. *Risk and Society*. Sage Publications Ltd.

Doyle, Gillian. 2002. *Media Ownership: The Economics and Politics of Convergence and Concentration in the UK and European Media*. Sage.

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

Fenton, Edited By Natalie. 2010. *New Media, Old News : Journalism & Democracy in the Digital Age*. London: Sage Publications Ltd.

Gates, Kelly, and Shoshana Magnet. 2007. "Communication Research and the Study of Surveillance." *The Communication Review* 10 (4): 277–293.

Goold, Benjamin, Ian Loader, and Angélica Thumala. 2013. "The Banality of Security The Curious Case of Surveillance Cameras." *British Journal of Criminology*: azt044.

Habermas, Jürgen, Sara Lennox, and Frank Lennox. 1974. "The Public Sphere: An Encyclopedia Article (1964)." *New German Critique* (3): 49–55.

Hewitt, Steve. 2008. *The British War on Terror: Terrorism and Counter-terrorism on the Home Front Since 9/11*. Continuum Intl Pub Group.

Hier, Sean P., Kevin Walby, and Josh Greenberg. 2006. "Supplementing the Panoptic Paradigm: Surveillance, Moral Governance and CCTV." *Theorizing Surveillance: The Panopticon and Beyond*: 23–45.

Hoskins, Andrew, and BEN O'LOUGHLIN. 2010. "Security Journalism and 'the Mainstream'in Britain Since 7/7: Translating Terror but Inciting Violence?" *International Affairs* 86 (4): 903–924.

Choudhury, Tufyal, and Helen Fenwick. 2011. "The Impact of Counter-terrorism Measures on Muslim Communities." *International Review of Law, Computers & Technology* 25 (3): 151–181.

Joinson, Monica Whitty And Adam. 2013. *Truth, Lies and Trust on the Internet*. Routledge Ltd.

Loader, Ian, and Neil Walker. 2007. *Civilizing Security*. Cambridge University Press.

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

Mansfeldova, Zdenka, Petra Guasti, aterina Vrablikova, and Jessie Hronesova. 2013. *D4.2 – Report on Perception of Security and Acceptance of Risk*. SECONOMICS "Socio-Economics Meets Security". Prague: Institute of Sociology, Academy of Sciences. http://www.seconomicsproject.eu/sites/default/files/content-files/deliverables/D4.2_Report_on_perception_of_security_and_acceptance_of_risk.pdf.

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

Monahan, Torin. 2011. "Surveillance as Cultural Practice." *The Sociological Quarterly* 52 (4): 495–508.

Neuman, W. Russell. 1992. *Common Knowledge: News and the Construction of Political Meaning*. University of Chicago Press.

Office, Great Britain: Cabinet. 2010. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. The Stationery Office.

Office, Home. 2009. *The United Kingdom's Strategy for Countering International Terrorism*. The Stationery Office.

Reid, Andrew A., and Martin A. Andresen. 2012. "An Evaluation of CCTV in a Car Park Using Police and Insurance Data." *Security Journal* (April 30).

Schlehahn, Eva, Marit Hansen, Jaro Sterbik-Lamina, and Javier Sempere Samaniego. 2013. "Report on Surveillance Technology and Privacy Enhancing Design". The Relationship Between Human Privacy And Security D 3.1. Surveillance, Privacy and Security: A Large Scale Participatory Assessment of Criteria and Factors Determining Acceptability and Acceptance of Security Technologies in Europe. Unabhängiges Landeszentrum für Datenschutz. http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf.

Stewart, Mark G., and John Mueller. 2011. "Cost-benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening." *Journal of Homeland Security and Emergency Management* 8 (1).

Temple, Mick. 2008. *The British Press*. Open University Press. https://www.dawsonera.com/abstract/9780335236954.

Tumber, Howard. 2001. "Democracy in the Information Age: The Role of the Fourth Estate in Cyberspace." *Information, Communication & Society* 4 (1): 95–112.

Wall, David S., and Matthew L. Williams. 2013. "Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing." *Policing and Society*: 1–4.

Annex: Coded Newspaper Articles

Stuxnet

Halliday, Josh 2010a. "Stuxnet worm is the 'work of a national government agency'". *The Guardian,* 24 September 2010.

Halliday, Josh 2010b. "Stuxnet worm is aimed to sabotage Iran's nuclear ambition, new research shows." *The Guardian,* 16 November 2010.

Halliday, Josh 2011. "WikiLeaks: US advised to sabotage Iran nuclear sites by German think tank." *The Guardian,* 18 January 2011.

Hopkins, Nick 2011. "Stuxnet attack forced Britain to rethink the cyber war". *The Guardian,* 30 May 2011.

Beaumont, Peter and Hopkins, Nick 2012. "US was 'key player in cyber-attacks on Iran's nuclear programme'". *The Guardian,* 1 June 2012.

Arthur, Charles 2013. "Symantec discovers 2005 US computer virus attack on Iran nuclear plants". *The Guardian,* 26 February 2013.

Beaumont, Claudine 2010. "Stuxnet virus: worm 'could be aimed at high-profile Iranian targets'". *The Daily Telegraph,* 23 September 2010.

Williams, Christopher 2011a. "Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel'". *The Daily Telegraph,* 21 January 2011.

Williams, Christopher 2011b. "Israel video shows Stuxnet as one of its successes". *The Daily Telegraph,* 15 February 2011.

"Iran accuses Siemens over Stuxnet cyber attack" 2011. *The Daily Telegraph,* 17 April 2011.

Williams, Christopher 2011c. "Stuxnet virus: US refuses to deny involvement". *The Daily Telegraph,* 27 May 2011.

Williams, Christopher 2012. "Barack Obama 'ordered Stuxnet cyber attack on Iran'". *The Daily Telegraph,* 1 June 2012.

Carmichael, Oliver 2012. "Flame and Stuxnet virus makers 'co-operated at least once'". *The Daily Telegraph,* 11 June 2012.

Glenny, Misha 2012. "The war being waged on the web". *The Daily Telegraph,* 17 July 2012.

CCTV

Lewis, Paul. 2010a. "Birmingham stops Muslim CCTV surveillance scheme". *The Guardian,* 17 June 2010.

Lewis, Paul. 2010b. "CCTV aimed at Muslim areas in Birmingham to be dismantled". *The Guardian,* 25 October 2010.

Travis, Alan. 2010. "Surveillance society soon a reality, report suggests". *The Guardian*, 11 November 2010.

Travis, Alan. 2011. "Whitehall admits CCTV faults as cameras continue to spread". *The Guardian,* 1 March 2011.

Lewis, Paul 2011. "You're being watched: there's one CCTV camera for every 32 people in UK". *The Guardian*. 2 March 2011.

Arthur, Charles 2012. "Trapwire surveillance system exposed in document leak". *The Guardian*, 13 August 2012.

Porter, Henry 2012. "Hi-def CCTV technology threatens our democracy – we must act now". *The Guardian*, 3 October 2012.

Watt, Holly 2010. "Police cameras to be regulated". *The Daily Telegraph*, 4 July 2010.

Paton, Graeme 2010. "CCTV 'used to monitor schoolchildren in toilets and changing rooms'". *The Daily Telegraph*, 28 December 2010.

Whiteheade, Tom and Kirkup, James 2011. "People get power to take CCTV abusers to court". *The Daily Telegraph*, 10 February 2011.

"Recording taxi conversations a 'staggering invasion of privacy'" 2011. *The Daily Telegraph*, 15 November 2011.

"Police to install CCTV in cars" 2012. *The Daily Telegraph*, 13 April 2012.

Swaine, Jon 2013. "Americans in favour of CCTV cameras in public places". *The Daily Telegraph*, 1 May 2013.

Body Scanners

Stratton, Allegra. 2010. "Full-body scanners being ordered for airports, says Gordon Brown". *The Guardian*, 3 January 2010.

Travis, Alan. 2010. "New scanners break child porn laws". *The Guardian,* 4 January 2010.

Williams, Zoe. 2010. "I'm all for privacy. But I don't want to seem like a Luddite". *The Guardian*, 6 January 2010.

Travis, Alan and Milmo, Dan 2010. "Airline passengers have 'no right' to refuse body scanners". *The Guardian*, 26 January 2010.

Travis, Alan 2010. "Anti-terror body scanners may be illegal, ministers warned". *The Guardian*, 16 February 2010.

Ludford, Sarah 2010. "European commission is fence-sitting on body scanners". *The Guardian*, 24 June 2010.

Pilkington, Ed 2010. "US airport security chiefs stand firm over invasion of the body scanners". *The Guardian*, 22 November 2010.

Bidder, Patrick 2011. "American ruling should revive body scanner debate in UK". *The Guardian*, 27 July 2011.

Coren, Victoria 2011. "Invasion of the body scanners". *The Guardian*, 2 October 2011.

Goodman, Amy 2012. "TSA scanners and the real risk of flying". *The Guardian*, 29 March 2012.

"Airport body scan images 'destroyed immediately' says Lord Adonis". *The Daily Telegraph*, 2 February 2010.

Pisa, Nick 2010. "Pope Benedict XVI criticises airport body scanners". *The Daily Telegraph*, 21 February 2010.

"Children will face airport body scanners". *The Daily Telegraph*, 30 March 2010.

Millward, David 2011. "New airport scanner which will take just five seconds". *The Daily Telegraph*, 6 June 2011.

"Doctor barred from flying after refusing body scan on health grounds". *The Daily Telegraph*, 30 June 2011

Sanchez, Raf 2012. "Ron Paul's son, Rand, detained at US airport". *The Daily Telegraph*, 23 January 2012.