Deliverable D6.1 – A report on resilience in "democratic" surveillance societies

Project acronym: IRISS
Project title: Increasing Resilience in Surveillance Societies
Project website: www.irissproject.eu
Project number: 290492
Programme: FP7-SSH-2011-2
Objective: To investigate societal effects of different surveillance practices from a multi-disciplinary social science and legal perspective.
Contract type: Small or medium-scale focused research project
Start date of project: 01 February 2012
Duration: 36 months

Co-ordinator: Trilateral Research and Consulting LLP
Dissemination level: PU
Deliverable type: Report
Version: This version of the report is a **DRAFT**. It is yet to be formally approved by the European Commission.
Submission date: 23 June 2014

Editors: *David Wright and Dr Rowena Rodrigues, Trilateral Research & Consulting LLP*

Contributors:

Professor Kirstie Ball, Open University

Dr Rocco Bellanova, Peace Research Institute Oslo

Dr Xavier L'Hoiry, University of Sheffield

Dr Richard Jones, University of Edinburgh

Dr Reinhard Kreissl, Institute for the Sociology of Law and Criminology (IRKS)

Charles Leleux, University of Stirling

Professor Clive Norris, University of Sheffield

Professor Charles Raab, University of Edinburgh

Dr Rowena Rodrigues, Trilateral Research & Consulting LLP

Dr Ivan Szekely, Eotvos Karoly Policy Institute, Hungary

David Wright, Trilateral Research & Consulting LLP

Dr. Nils Zurawski, University of Hamburg

Contents

List of figures

List of tables

1 INTRODUCTION

This report presents a review of the current thinking on resilience. It examines how resilience is used in different contexts and selected domains. The domains examined include: European Commission, UK Cabinet Office, [dictatorial and] post-dictatorial regimes, US cyber security and critical infrastructure protection, the UN, transport, civil protection, the banking sector and critical infrastructures (telecommunications networks). A horizontal analysis of resilience shows the commonalities and differences in the definitions of resilience, features and elements of resilience, advantages of resilience, the elements of a resilience strategy, who should employ it and in what circumstances, followed by some propositions for resilience in a surveillance society.

The report also examines how the open nature of democratic societies can make them more vulnerable to attacks on infrastructures or people and how, at the same time, it can make them more resilient to those attacks in terms of social, economic and institutional responses. To this end, the report examines two diverse sets of adverse events (in the first group are one-off events, with a shock or shocking impact – or a series of the same kind of events that are sudden, devastating, hazardous, violent or catastrophic; in the second group are stressing events that continue for some period of time, and share the following features or characteristics: they involve the collection of data in vast amounts, they are objects of public debate, they may represent infringements on existing rights, they are long-lasting, consisting of processes that encompass various social and political actors). Each of the adverse events are analysed in relation to their nature, institutional, social and economic and media responses and from the IRISS project perspective.

The report examines the notion of surveillance and, in particular, resilience in a surveillance society and whether resilience offers a useful strategy for countering the negative effects of surveillance in undermining the freedoms and values that underpin a democracy. It also identifies measures to increase resilience in a surveillance society. The report also distils lessons for resilience from work packages 3-5 of the IRISS project.

1.1 OBJECTIVES

The objectives underlying this report are to:

1. Examine how the open nature of democratic societies can make them more vulnerable to attacks on infrastructures or people and how, at the same time, it can make them more resilient to those attacks in terms of social, economic and institutional responses.
2. Identify options for enhancing social, economic, institutional resilience based on a comparative analysis of past and current experiences in Europe and elsewhere.

This report considers the challenges raised by surveillance in the context of economic, social and institutional factors and the resilience options as prospective responses. Economic actors use surveillance systems and technologies to protect critical infrastructures as well as private enterprise. Society faces the ubiquity of surveillance

in the daily lives of the populace. Institutions must deal with the challenges raised by surveillance, both as a means of protecting citizens but also in ensuring that surveillance does not undermine the fundamental values these institutions are supposed to protect.

1.2 OVERVIEW

The concept of resilience is typically used in relation to terrorism, criminal threats or natural or man-made disasters to which individuals, societies, and communities are vulnerable. Surveillance can play a part in such resilience strategies, and can contribute to enhancing safety and security, whether by preventing or detecting harmful acts.

However, IRISS is particularly and uniquely concerned with understanding and increasing the resilience of society to *surveillance* itself. Such an approach adapts concepts and terms that already figure in studies of resilience, but applies them here in a novel context: the threats posed by surveillance.

Surveillance – whatever its benefits in coping with the kinds of threat mentioned above – may itself pose a threat to individuals, societies, and communities because of its ubiquity, intensity, and use of personally identifiable information. These qualities of surveillance may erode privacy and a host of freedoms, rights, and values that it is designed to protect, including democracy itself. This gives surveillance a negative connotation in the eyes of many. But we lack understanding of how best to respond to the threat posed by surveillance. The concept of resilience may generate tools for analysing and for acting to mitigate such a threat.

The use of the conceptual terminology of resilience in relation to *security* threats typically involves, for example, identification of the weaknesses and failures of current defences and an assessment of the risk caused by the threats, with a view to mitigating vulnerability and reducing risk. This may involve a searching examination of the weakness or absence of political, social, economic, psychological, material, military and other infrastructures in the face of particular security threats. In fact, resilience measures often do involve a variety of forms of surveillance to detect and counter the security threat.

However, if we shift the focus to how society (individual, community) can be resilient to *surveillance* itself, measures would similarly involve not only *responses* to surveillance but also *anticipatory* activities to prevent or to minimise the implementation of surveillance measures. One of these activities would be a closer examination of the resources that may be absent or adversely impacted by particular forms of surveillance.

What do we mean by "resilience"?[1] Although this varies according to the domain in question, an initial literature review suggests some common conceptual language on

[1] This was discussed at the Meeting of the IRISS Advisory Group in Brussels, 24 January 2013. We acknowledge in particular the contribution made by Roger Clarke to the clarification of this concept. See his paper: Clarke, Roger, "The Resilience of Society in the Face of Surveillance", Notes of 5 February 2013 for the Advisory Board of the IRISS project, 2013. http://www.rogerclarke.com/DV/IRISSR.html

which to draw. A document on food security defines it in that context as "the capacity of agricultural development to withstand or recover from stresses and shocks and thus bounce back to the previous level of growth."[2] Cognisant of that document, another document in the same field says, more generally: "Resilience is the ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks."[3] It continues:

> The concept of resilience has two dimensions: the inherent strength of an entity – an individual, a household, a community or a larger structure – to better resist stress and shock and the capacity of this entity to bounce back rapidly from the impact. […] It requires **a multifaceted strategy** and a broad systems perspective […and] calls for a **long-term approach**.[4]

In addition we recognise that resilience is also conceptualised as forward-looking, in order "to anticipate, prepare for, and, as far as possible, avoid the worst excesses of the next disruption"[5]

Steps to be taken to build resilience often include: *anticipate*, *survey*, *prevent*, *tolerate*, *recover*, *restore* and *learn*. These roughly parallel a temporal sequence.[6] The concept of *vulnerability* is also important in relation to resilience. It has been defined as "The conditions determined by physical, social, economic, and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards."[7]

A heuristic diagram[8], illustrated below, is drawn from work on agricultural development. It is useful in showing the general definition of resilience—involving both preparedness and response—and the part played by the concepts "stress" and "shock". Although we will supersede this diagram with one that is more appropriate to IRISS, it is useful to examine the agricultural development diagram and its definitions.

---

[2] The Montpellier Panel, *Growth with Resilience: Opportunities in African Agriculture*, Agriculture for Impact, London, 2012, p. 11.

[3] European Commission, *Communication from the Commission to the European Parliament and the Council – The EU Approach to Resilience: Learning from Food Security Crises*, COM(2012) 586 Final, Brussels, 3.10.2012, p. 5.

[4] European Commission, *Communication from the Commission to the European Parliament and the Council – The EU Approach to Resilience: Learning from Food Security Crises*, COM(2012) 586 Final, Brussels, 3.10.2012, p. 5; emphases in original.

[5] Cho, Albert, Simon Willis and Martin Stewart-Weeks, *The Resilient Society: Innovation, Productivity, and the Art and Practice of Connectedness,* Cisco Internet Business Solutions Group (IBSG), 2011.

[6] The Montpellier Panel, *Growth with Resilience: Opportunities in African Agriculture*, Agriculture for Impact, London, 2012, p. 11. Other terms include *withstand, resist, handle, absorb, adapt, response, resume, optimise, innovate, reconstruct, renew, persist.*

[7] International Strategy for Disaster Reduction (ISDR), *Living with Risk: A Global Review of Disaster Reduction Initiatives*, 2004 Version, Volume I, United Nations: New York and Geneva, 2004, http://www.unisdr.org/files/657_lwr1.pdf, accessed 9 March 2013, p. 16.

[8] Adapted from The Montpellier Panel, *Growth with Resilience: Opportunities in African Agriculture*, Agriculture for Impact, London, 2012, p. 11. This diagram was slightly adapted from Conway, Gordon, Jeff Waage and Sara Delaney, *Science and Innovation for Development*, UK Collaborative on Development Science, London, 2010, p. 309.
http://www.ukcds.org.uk/_assets/file/book/science_innovation_book_lowres.pdf

In this construct, "stress" is defined as "a regular, sometimes continuous, relatively small and predictable disturbance"[9] and a "shock" as "an irregular, relatively large and unpredictable disturbance".[10] Although for our purposes, it would be advisable to disaggregate these definitions in order to distinguish between size, predictability and continuity, they are but some of the concepts that have already been shown to be useful in other domains of resilience.

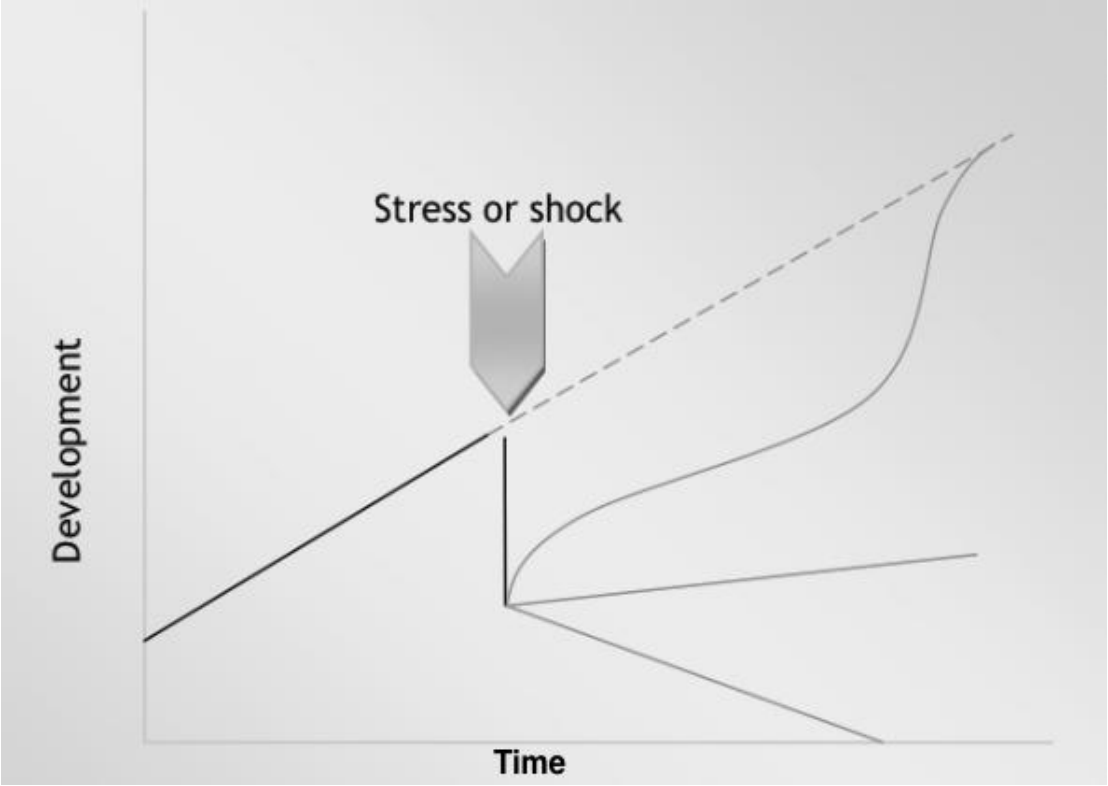

Figure 1 Agricultural development model of resilience

The innovation of IRISS is to model an approach to resilience to surveillance drawing from such terminology. The IRISS model suggests that increasing societal resilience to surveillance would best be conceived as a continuous process embracing anticipatory, preventive measures to mitigate the harms that may be brought about through surveillance; measures to absorb, resist or withstand the threats posed by surveillance; as well as post-event measures to recover and to learn how better to anticipate and/or to cope with harmful surveillance. Resilience is therefore not a one-off approach, but a sustained and systematic process that includes capacity-building institutional and procedural development. It incorporates "resistance" – a relatively unexamined concept in surveillance studies, involving individual and group opposition, protest, and defensive measures – but is not synonymous with it.[11]

[9] The Montpellier Panel, *Growth with Resilience: Opportunities in African Agriculture*, Agriculture for Impact, London, 2012, p. 11.
[10] Ibid.
[11] In this respect, perhaps the following are relevant from the Special issue, Surveillance and Resistance of Security and Society, *Surveillance and Society,* Vol. 6, No. 3, 2009: Fernandez, Luis and Laura Huey, "Is Resistance Futile? Thoughts on Resisting Surveillance", pp. 199-202; Martin, Aaron, Rosamunde van Brakel and D. Bernhard, "Understanding resistance to digital surveillance: Towards a multidisciplinary, multi-actor framework", pp. 213-232; Introna, Lucas, and Amy Gibbons,

This revised model, shown in the schematic diagram (Figure 2) below, depicts two axes: social values, and time. "Social values" can refer to freedoms, liberties, rights, democracy, security etc. The diagram shows a series of stresses, each one followed by an episode of resilience, which in the paradigm case restores the social value in question to its prior state. The diagram also shows a final stress or shock, which could be either small or large, but in either case has a larger effect on social values, so that the resilience phase has a more uncertain outcome, and may take a longer period of time. The uncertainty of the outcome is shown in the diagram by the top line following the "final" stress or shock; and two further lines that may represent the reestablishment of social values at reduced levels.[12]

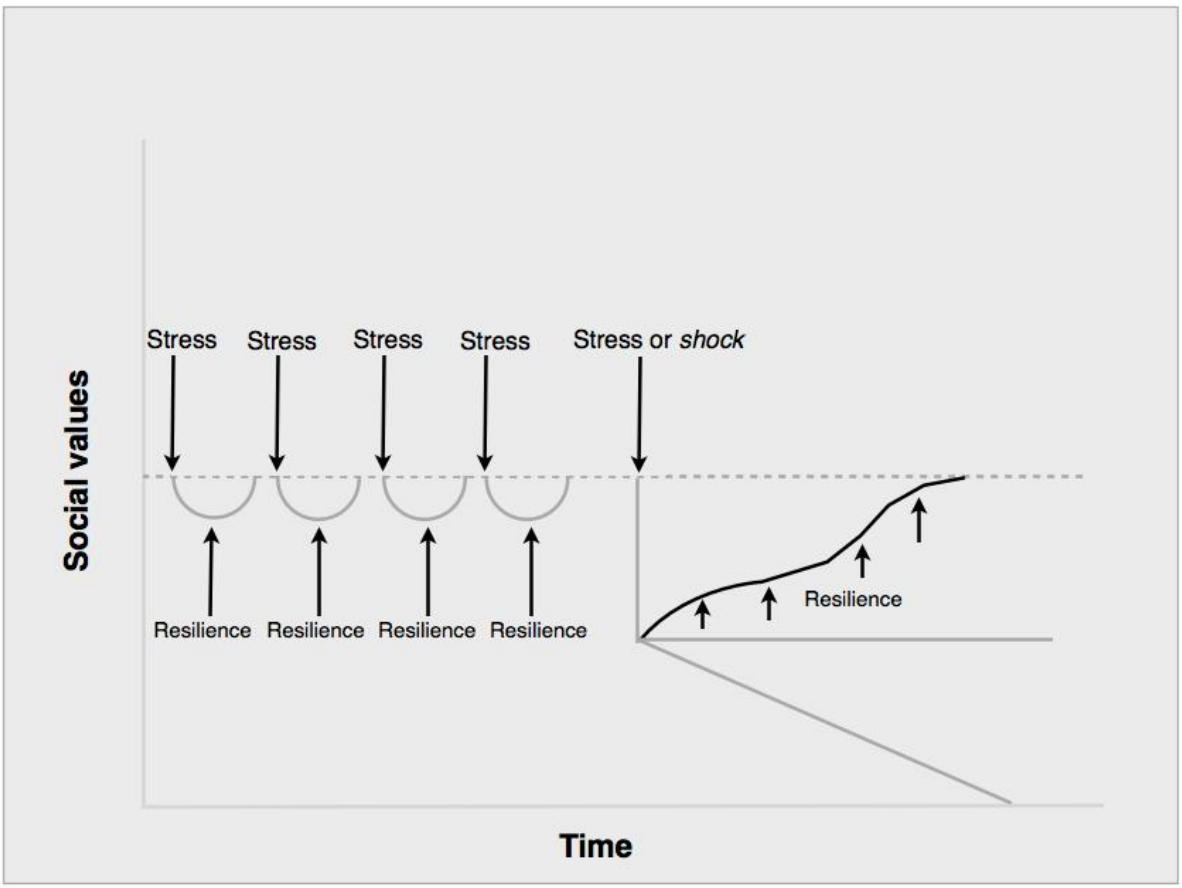

Figure 2 IRISS model of resilience

Whereas Figure 1 models resilience in the face of the occurrence of a single major event, Figure 2 models resilience both in the face of incremental, "creeping" threats to social values, as well as in relation to a single major event or a small but culminating

"Networks and Resistance: Investigating online advocacy networks as a modality for resisting state surveillance", pp. 233-258; Wells, Helen, and David Wills, "Individualism and Identity: Resistance to Speed Cameras in the UK", pp. 259-274; and Sanchez, Andrés, "Facebook Feeding Frenzy: Resistance-through-Distance and Resistance-through-Persistence in the Societied Network", pp. 275-293. See also Bennett, Colin J., *The Privacy Advocates: Resisting the Spread of Surveillance*, MIT Press, Cambridge, MA, 2008.

[12] For the sake of simplicity the values are depicted as fully restored after stresses (except for the ultimate stress or shock), but it is possible to envisage other trajectories: one in which the values are eroded over time (the line descends); or alternatively societal values are actually enhanced (the line ascends).

event that "breaks the camel's back". Figure 2 thus models resilience in relation to *surveillance*, in which surveillance threats may be "creeping" and gradual, or sudden and dramatic. It should be noted however that the model in Figure 2 is a general one, and is potentially also applicable to *security* threats.

There are a number of benefits of adopting a resilience model to the threats posed by surveillance:

- it helps both organise existing knowledge, and indicate gaps
- it suggests strategies and tactics and helps to evaluate existing ones
- it shows the relationship between, and ways of integrating, different resilience instruments
- the model can be applied at many different levels, from the local to the global

We particularly recognise the potential of the concept of "resilience" to become, as Béné et al. put it, a "form of integrating discourse" able to rally an "increasing number of people, institutions, and organisations under its banner, as it creates communication bridges and platforms between disciplines and communities of practices, and offers common grounds on which dialogue can then be initiated between organisations, departments or ministries which had so far very little, or no history of collaboration".[13] Such bridges and platforms are crucial to countering the detrimental effects of surveillance, ensuring effective respect for the societal values and principles and at the same time protecting people and communities.

In line with this approach, a host of questions can be asked; among many others, these include:

- How and why, for instance, is a society's political system vulnerable to calls for greater surveillance by law enforcement agencies?
- What is the state of public opinion and the media about the acceptability of what kind, level, and duration of surveillance?
- How capable, willing, and connected are civil liberty and advocacy groups to promote resilience to surveillance, whether by learning about surveillance threats early enough; by opposing or by mitigating proposed surveillance policies and measures; or by challenging those that are already in place?
- How robust are anti-surveillance legal or other regulatory rules and safeguards?
- How can privacy impact assessment (PIA) or "surveillance impact assessment" help in resilience to surveillance?
- Are risks to privacy, human rights and freedoms well conceptualised so that, for instance, small and large threats are not treated identically by tactics and strategies for resilience to surveillance?
- If not, is this conceptual weakness itself a vulnerability?
- What are the conditions that increase a society's susceptibility to the impact of surveillance once it has happened?
- More abstractly, are there usable concepts of *stress* and *shock* to apply to the case of resilience to surveillance; and concretely, can individuals,

[13] Béné, Christophe, Rachel Godfrey Wood, Andrew Newsham and Mark Davies, "Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes", IDS Working Paper 405, September 2012.

communities, and societies organise themselves and learn sufficiently to prevent surveillance stresses from becoming surveillance shocks?

- Must we remain with "slippery slope" scenarios, in which any small incursion on privacy or freedoms must mobilise maximal opposition?
- On the other hand, how, and at what speed, can an individual, community or society recover from a surveillance threat/attack and learn lessons from it?
- What multifaceted strategies can be devised for resilience to surveillance, "aimed at both reducing the multiple risks of a crisis and at the same time improving rapid coping and adaptation mechanisms"?[14]
- What long-term strategies can be devised for resilience to surveillance, "based on alleviating the underlying causes conducive to crises, and enhancing capacities to better manage future uncertainty and change"?[15]
- What are the barriers to resilience in surveillance societies?

2 A REVIEW OF CURRENT THINKING ON RESILIENCE

The term resilience is defined and used in various ways in different fields. This section conducts a literature review to determine how resilience is used in different domains to determine and draw conclusions about how resilience is conceptualised and to outline options for improving resilience of critical infrastructure, enterprise and society.

2.1 ANALYSIS OF DIFFERENT DOMAINS AND CONTEXTS

In this section we analyse the following: European Commission and resilience, UK Cabinet Office and resilience, resilience in [dictatorial and] post-dictatorial regimes, resilience in the US (cyber security and critical infrastructure protection), the UN and resilience, resilience and transport, civil protection in the European context, resilience in the banking sector and critical infrastructures (resilience and telecommunications networks). The analysis of the domains and contexts broadly focuses on the following aspects (though there are some variations in how the coverage):

- how the term 'resilience' is defined and used
- the rationale and justifications for using the concept
- Characteristics or features of the concept
- Policy aspects and/or strategic aspects of resilience (what are the elements in using resilience as a strategy?)
- Analysis from an IRISS perspective (lessons for IRISS resilience strategy, applicability or relevance to our strategy for resilience in a surveillance society).

[14] European Commission, *Communication from the Commission to the European Parliament and the Council – The EU Approach to Resilience: Learning from Food Security Crises*, COM(2012) 586 Final, Brussels, 3.10.2012, p. 5.

[15] European Commission, *Communication from the Commission to the European Parliament and the Council – The EU Approach to Resilience: Learning from Food Security Crises*, COM(2012) 586 Final, Brussels, 3.10.2012, p. 5.

2.1.1 European Commission and resilience

Dr Rowena Rodrigues, Trilateral Research & Consulting

Definition and use of the term

The European Commission has used the term "resilience" in various contexts, including in relation to critical infrastructures, systems (networks, information systems) and in relation to the individual, community, country or region. The Critical Information Infrastructure Protection (CIIP) Communication of 30 March 2009,[16] its Accompanying Document[17] and the CIIP Achievements Communication[18] speak of the resilience of critical information infrastructures (CII). The European Principles and Guidelines for Internet Resilience and Stability speak of resilience in relation to systems.[19] The Cybersecurity Strategy[20] and the Proposal for a Network Security Measures Directive focus on resilience in network and information systems.[21] The Communication on the EU Approach to Resilience focuses on resilience of the "individual, community, country or region".[22]

Resilience is also linked to other important concepts. For instance, resilience is linked to security – this is a prominent linkage featured in a large number of EC documents.[23] In addition, it is linked to stability.[24]

---

[16] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 30 March 2009 on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009) 149 final, Brussels, 30.3.2009.

[17] European Commission, Accompanying document to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience", Commission Staff Working Document, SEC(2009)400, Brussels, 30.3.2009.

[18] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security', COM(2011) 163 final. Brussels, 31.03.2011.

[19] European Commission, European Principles and Guidelines for Resilience and Stability of the Internet, March 2011. http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf

[20] European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, Brussels, 7.2.2013. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_fr.pdf

[21] European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, Brussels, 3.10.2012.

[22] European Commission, Communication from the Commission to the European Parliament and the Council, The EU Approach to Resilience: Learning from Food Security Crises, COM(2012) 586 final, Brussels, 3.10.2012.

[23] These include: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe, COM(2010) 245 final, Brussels, 19.5.2010; European Commission, EUROPE 2020: A strategy for smart, sustainable and inclusive growth, COM(2010) 2020 final, Brussels, 3.3.2010; European Commission, CIIP Communication 2009; European Commission, Accompanying document to CIIP Communication 2009.

Rationale and justification

The various EC documents examined indicate the following rationales and justifications for resilience:

- To secure against vulnerabilities, threats, risks, attacks
- To strengthen the economy
- To strengthen the development process
- To improve the cost effectiveness of a resilience-based approach.[25]

Although there are various EC Communications and other documents that mention resilience, many of them do not define or specify what they mean by the term. The EC Communication on the EU Approach to Resilience, however, defines resilience as "the ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks".[26] Resilience, in this postulation, has two dimensions: the inherent strength of an entity and the capacity to bounce back from impact.

Another EC document (the European principles and guidelines for the resilience and stability of the Internet) adopts the ENISA definition of resilience, i.e., the ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional or naturally caused) affecting normal operation.[27] The CIIP Communication of 30 March 2009 calls security and resilience of critical information infrastructures as "the frontline of defence" against failures and attacks.

So against what is resilience addressed? Various EC documents use different terms. For example, the CIIP Communication 2009 and its Accompanying Document speak of resilience against *failures and attacks* (they also mention *risks* and *disruptions*). The EU Strategy for supporting disaster risk reduction focuses on enhancing resilience against *disasters and hazards*.[28] The Digital Agenda for Europe[29] and the European principles and guidelines for the resilience and stability of the Internet[30] speak of being resilient against *threats* (such as spam, identity theft, online fraud, cyber attacks). The Europe 2020 Strategy and the Proposal for a Network Security Measures Directive talk about resilience against *risks.*[31] The Communication on the

---

'Achievements and next steps: towards global cyber-security', COM(2011) 163 final. Brussels, 31.03.2011.

[24] As in European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, Brussels, 3.10.2012.

[25] European Commission, Communication from the Commission to the European Parliament and the Council, The EU Approach to Resilience: Learning from Food Security Crises, COM(2012) 586 final, Brussels, 3.10.2012.

[26] European Commission, *The EU Approach to Resilience,* op. cit. 2012.

[27] ENISA, Glossary. http://www.enisa.europa.eu/act/res/files/glossary

[28] European Commission, Communication from the Commission to the Council and the European Parliament - EU Strategy for supporting disaster risk reduction in developing countries, COM (2009) 84, Brussels, 23.02.2009

[29] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe, COM(2010) 245 final, Brussels, 19.5.2010.

[30] European Commission, European Principles and Guidelines for Resilience and Stability of the Internet, op. cit., 2011.

[31] European Commission, Europe 2020 Strategy and the Proposal, op. cit., 2012

EU Approach to Resilience focuses on resilience against *stresses and shocks, crisis, uncertainty* and *change.*[32]

Characteristics or features or elements of resilience

From an examination of the various documents charting the European Commission's perspectives on resilience, we derive several core features or elements of resilience:

1. Anticipation of vulnerabilities, threats, attacks, crises
2. Preparedness
3. Prevention, detection and response
4. Mitigation
5. Recovery
6. Sharing of responsibility and co-operation between stakeholders.

Policy aspects

Cyber resilience is a strategic EC priority. For instance, the Proposal for a Network Security Measures Directive states

> The resilience and stability of network and information systems is therefore essential to the completion of the Digital Single Market and the smooth functioning of the Internal Market. The likelihood and frequency of incidents and the inability to ensure efficient protection also undermine public trust and confidence in network and information services.[33]

The strategic and policy focus on cyber resilience is also evident in the activities of ENISA[34] and the European Public-Private Partnership for Resilience (EP3R).[35]

Another priority is Chemical, Biological, Radiological and Nuclear (CBRN) resilience, as evident in the EU CBRN Communication and Action Plan[36] which calls for co-ordinated action to prevent, detect, prepare and respond to CBRN incidents and the EU CBRN Resilience Programme.[37]

Resilience has, of late, become a more visible (or explicit) thrust in EU security research. The European Commission FP7 2013 Security Work Programme,[38] while exhorting that proposed security solutions pay attention to societal impact, calls for the development of solutions that strengthen societal resilience and active

---

[32] European Commission, Communication on the EU Approach to Resilience, op. cit., 2012.
[33] European Commission, 2012, op. cit., 24.
[34] See ENISA, Resilience and CIIP. http://www.enisa.europa.eu/activities/Resilience-and-CIIP
[35] ENISA, European Public-private Partnership for Resilience. https://resilience.enisa.europa.eu/ep3r
[36] European Commission, Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, COM(2009) 273 final, Brussels, 24.6.2009. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/com_2009_0273_en.pdf
[37] See European Commission Home Affairs, Securing Dangerous Material. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/securing-dangerous-material/index_en.htm
[38] European Commission C (2012) 4536 of 09 July 2012, OJ C202 of 10 July 2012. http://ec.europa.eu/research/participants/portal/page/cooperation;efp7_SESSION_ID=3JzGQB7McpcQMv1jQHwQnypGQYbhTsJf5WMrDPJxmm7fv2p7J2BL!4432079?callIdentifier=FP7-SEC-2013-1#wlp_call_FP7

participation of citizens as security enhancing resources. *Societal resilience*, as a policy thrust, is deeply embedded in this Work Programme. The European Commission's 2012 Security Work Programme particularly encourages research proposers to "to develop solutions strengthening societal resilience and active participation of citizens as security enhancing resources".[39] Cyber resilience is a major thrust. The Security Work Programme makes several references to resilience in relation to crisis response.

Resilience was also a key thrust in the Commission's Socio-Economic Sciences and the Humanities (SSH) Work Programme of 2012,[40] which was released in July 2011 and which called for the establishment of new mechanisms to "reinforce economic policy coordination needed to ensure the EU is more resilient, and able to effectively prevent major economic instabilities in the future".[41] The SSH Work Programme of 2012[42] focused on citizens' resilience in times of crises. It suggests that "understanding how citizens claim and enact their rights and how they develop resilience in difficult times is crucial for both the EU and its Member States" (Activity 8.5: The Citizen in the European Union). The 2011 SSH Work Programme, released 20 July 2010,[43] speaks of resilience to external economic shocks in the context of developing countries. The IRISS consortium successfully responded to a call in this Work Programme (Topic SSH.2011.5.1-2) which postulated the concern that "the open nature of democratic societies can make them more vulnerable to attacks on infrastructures or people; at the same time it can make them more resilient to those attacks in terms of social, economic and institutional responses" and which asked for the identification of options for enhancing social, economic, institutional resilience based on a comparative analysis of past and current experiences in Europe and elsewhere.

Thus, we see an increasing, explicit focus on resilience in EC research calls. There were and are various projects focussing on resilience such as IRISS (Increasing Resilience in Surveillance Societies), CIPRNET (Critical Infrastructure Preparedness and Resilience Research Network), PRACTICE (Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment), RIBS (Resilient Infrastructure and Building Security), SECCRIT (SEcure Cloud computing for CRitical infrastructure IT), MULTISENSE CHIP (The lab-free CBRN detection device for the identification of biological pathogens on nucleic acid and immunological level as a lab-on-a-chip system applying multi-sensor technologies).

Various FP7 ICT projects such as TCLOUDS (Trustworthy Clouds Privacy and Resilience for Internet-scale Critical Infrastructure), AMBER (Assessing, measuring, and benchmarking resilience), INSPIRE (Increasing security and protection through infrastructure resilience), SERSCIS (Semantically Enhanced Resilient and Secure Critical Infrastructure Services), INTERSECTION (Semantically Enhanced Resilient

[39] ftp://ftp.cordis.europa.eu/pub/fp7/docs/wp/cooperation/security/k-wp-201201_en.pdf
[40] FP7-SSH-2012-2. European Commission C (2011)5068 of 19 July 2011.
[41] OJ C213 of 20 July 2011.
http://ec.europa.eu/research/participants/portal/page/call_FP7?callIdentifier=FP7-SSH-2012-2&specificProgram=COOPERATION#wlp_call_FP7
[42] European Commission C (2012) 4536 of 09 July 2012.
[43]http://ec.europa.eu/research/participants/portal/page/call_FP7?callIdentifier=FP7-SSH-2011-2&specificProgram=COOPERATION#wlp_call_FP7

and Secure Critical Infrastructure Services), TRESPASS (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security) also focus on aspects of resilience.

Analysis from an IRISS perspective (lessons for resilience strategy)

From our initial review of EC documents, we have identified various elements that could be part of a resilience strategy. In order to make systems, individuals or groups (e.g., society) resilient, measures that would contribute to a more robust resilience strategy include the following:

1. Policy dialogue
2. Good risk management and sound risk methodologies and vulnerability assessment
3. Standardisation
4. Increased transparency
5. Regional and/or international approach to resilience rather than only a national approach
6. Multi-stakeholder approach
7. Stakeholder collaboration and co-ordination
8. Flexibility
9. Innovation.

References

European Commission, Accompanying document to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience", Commission Staff Working Document, SEC(2009)400, Brussels, 30 March 2009.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2009:0400:FIN:EN:DOC

European Commission, Commission staff working paper accompanying the Commission Communication - Ensuring efficient, safe and sound derivatives markets, COM(2009) 332 final, Brussels, 3 July 2009.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009SC0905:EN:HTML

European Commission, A strategy for a Secure Information Society - "Dialogue, partnership and empowerment", Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions, COM(2006) 251 final, Brussels, 31 May 2006.

European Commission, EU Strategy for supporting disaster risk reduction in developing countries, Communication from the Commission to the Council and the European Parliament, COM (2009) 84, Brussels, 23 Feb 2009.

European Commission, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", Communication from

the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 30 March 2009 on Critical Information Infrastructure Protection, COM(2009) 149 final, Brussels, 30 March 2009.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:NOT

European Commission, A Digital Agenda for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 245 final, Brussels, 19 May 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245:EN:NOT

European Commission, 'Achievements and next steps: towards global cyber-security', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM(2011) 163 final. Brussels, 31 Mar 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0163:EN:NOT

European Commission, The EU Approach to Resilience: Learning from Food Security Crises, Communication from the Commission to the European Parliament and the Council, COM (2012) 586 final, Brussels, 3 Oct 2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0586:FIN:EN:HTML

European Commission, Consultation Document: Possible initiatives to enhance the resilience of OTC Derivatives Markets, Commission Staff Working Paper, SEC (2009) 914 final, Brussels, 3 July 2009.
http://ec.europa.eu/internal_market/consultations/docs/2009/derivatives/derivatives_consultation.pdf

European Commission, EUROPE 2020: A strategy for smart, sustainable and inclusive growth, COM (2010) 2020 final, Brussels, 3 March 2010.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC2020:EN:NOT

European Commission, European Principles and Guidelines for Resilience and Stability of the Internet, 2011.
http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf

European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013) 1 final, Brussels, 7 Feb 2013.
http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_fr.pdf

European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and

information security across the Union, COM(2013) 48 final, Brussels, 3 Oct 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF

European Commission, Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, COM(2009) 273 final, Brussels, 24 June 2009. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/com_2009_0273_en.pdf

2.1.2 UK Cabinet Office and resilience

Dr Richard Jones and Professor Charles Raab, University of Edinburgh

The UK's Cabinet Office is a UK Government department whose official role is to support the Prime Minister and his or her Cabinet (i.e., the most senior ministers) and "ensure the effective running of government".[44] In recent practice, however, its more particular role has been to take responsibility for areas of government not easily fitting in one of the other governmental departments; to co-ordinate activities between government departments; and (in recent years) to lead on constitutional reform and on civil service efficiency delivery. The Cabinet Office's areas of activity of greatest interest to IRISS are probably "National Security", "Public safety and emergencies", "Defence and armed forces" and, to a lesser extent, "Foreign affairs" and "Community and society".

In the area of "National Security", for example, the Cabinet Office has developed policies in relation to UK cyber-security, counter-terrorism and responding to emergency situations. It offers detailed guidance on topics such as the UK's "Local resilience forums" and on "Surveillance and counter-terrorism".[45] In the area of "Public safety and emergencies", the Office has developed plans in relation to "Working with local partners to plan for, and respond to, emergencies", "Planning for health emergencies", and "Improving the UK's ability to absorb, respond to, and recover from emergencies". Detailed guidance is offered on topics such as "Pandemic flu", "Resilience in society" and "Risk assessment: how the risk of emergencies in the UK is assessed". The Civil Contingencies Act 2004 provides much of the legislative background.

Not only does the Cabinet Office take the lead in areas of interest to IRISS, but also it makes frequent reference to the terms "resilience" and "resilient". One could perhaps characterise the Office's role in the various areas in which it is involved as including helping to co-ordinate activities between different branches of UK government, both at a national and a local level; developing "best practice" guidance and overseeing training and exercises; and disseminating relevant information, both in terms of general government policy and planning in each area, and in terms of specific scientific or other substantive information. The approach to 'integrated emergency management' (IEM) describes the elements of resilience in saying, in a guidance

[44] UK Cabinet Office. https://www.gov.uk/government/organisations/cabinet-office
[45] UK Cabinet Office. https://www.gov.uk/government/topics/national-security

document, that IEM "includes anticipation, assessment, prevention, preparation, response and recovery. Resilience is about all these aspects of emergency management, and this guide deals with the resilience of existing entities the UK such as buildings, systems and networks."[46]

Among the ways it disseminates information and plans is by publishing its numerous plans, overviews, policies and other documents in PDF format on its extensive website. These are publicly available documents, and hence a potentially useful resource from an analytic perspective. The intended use of the various documents, presumably, is by relevant parts of government (though also the private sector and members of the public) that can download the documents, study them, implement policy in line with the guidance, or at least understand government policy in each area. Some documents are classified (i.e., not publicly available) though there remains a significant volume of publicly available documentation. Its website is searchable, and a search for the terms "resilience" or "resilient" returns a large number of results relating to policies, areas of responsibility and specific documents.

In order to illustrate how the term "resilience" is used and understood by the Cabinet Office, we present three selected examples drawn from different topic areas.

Illustrative examples

The first example is the area of cyber security. In February 2013, the Cabinet Office published on its website a summary of policy in that area, entitled "Keeping the UK safe in cyber space".[47] The policy summary includes links to prior official publications, but can also be added to with subsequent materials. The word "resilient" appears three times in the policy overview text, as in the phrase, "the government must look at new ways to protect businesses and make the UK more resilient to cyber-attacks and crime". [48] Among the key documents to which the page links is the UK Cyber Security Strategy, also published by the Cabinet Office in late 2011. That document mentions "resilience" or "resilient" 18 times. One of the four principal objectives of the strategy is, "Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace".[49] In other occurrences the term often appears alongside the words "safe" and/or "secure".

The meaning of the term "resilience" is not clearly defined, but in relation to this subject area would appear to refer to two matters of particular importance. The first is "resilience" in the sense of offering "protection" from possible cyber attacks; and the second is "resilience" in the sense of "business continuity" (meaning having the capability to provide uninterrupted services, or at least to minimise server "downtime"). Returning to the policy summary on their website, it can be seen that one of the Action headings has the aim of "[making] the UK more resilient to cyber-

[46] UK Cabinet Office, *Resilience in society: infrastructure, communities and businesse s– How networks and individuals can support the country's emergency planning, response and recovery, and keep systems and services running*, 20 February 2013. https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses

[47] UK Cabinet Office, "Keeping the UK safe in cyber space". https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

[48] Ibid.

[49] Cabinet Office, *UK Cyber Security Strategy*, London, Cabinet Office, 2011.

attacks". Action points under this heading include establishing a UK-wide fast response team "to improve national co-ordination of cyber incidents"; "[setting] up a new Cyber Incident Response scheme in GCHQ to help organisations recover from a cyber security attack"; extending the remit of the Centre for the Protection of National Infrastructure,[50] asking it to work "with all organisations that may have a role in protecting the UK's critical systems and intellectual property"; and the setting up of "a national cyber crime unit". All of these are organisational changes, yet important ones, and the use of the term "resilient" serves both to justify such changes (and possibly additional expenditure) and to connote a certain "strength" about the measures.

The second example area is that of "community resilience", a programme launched in 2008. In 2011 the Cabinet Office published a document entitled the Strategic National Framework on Community Resilience.[51] The document "explores the role and resilience of individuals and communities before, during and after an emergency". [52] At the start of the document, a definition of "resilience" (drawn from an earlier source) is offered, namely, "The capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure, and identity".[53] (Later, additionally, the document notes that, "Sir Michael Pitt defines resilience as: "The ability of a system or organisation to withstand and recover from adversity.""[54]) "Community resilience", more specifically, is defined as, "Communities and individuals harnessing local resources and expertise to help themselves in an emergency, in a way that complements the response of the emergency services."[55] The document explains that it sets out ways the Government can "contribute to building and enhancing community resilience in the UK".[56] The aim seems to be to encourage individuals and communities to prepare for such emergencies as "coastal flooding, flu pandemics and attacks on the transport system", and to work better alongside the emergency services and other authorities. Participation in the programme is voluntary, and government's role is as a facilitator.

Whereas, sociologically, one can imagine "community resilience" referring to some aspect of "social bonds" (similar to "social capital", for example) better unifying a community so that it is more united in the face of an emergency event, here the term is used more to connote preparedness, practicalities, liaison with the emergency services, and preparedness involvement. As such, the programme seems consistent with both the earlier Labour Government's various attempts at what David Garland has termed "responsibilisation"[57], and with Conservative Prime Minister David Cameron's notion of "the Big Society". The term "resilience" here, therefore, refers primarily to disaster recovery. Additionally, at first blush, it contains an almost

[50] The Centre for the Protection of National Infrastructure (CPNI) works alongside the UK's Security Service (MI5).
[51] Cabinet Office, *Strategic National Framework on Community Resilience*, London, Cabinet Office, 2011.
[52] Ibid., p. 3.
[53] Ibid., p. 4. The original source of the definition is given as Charlie Edwards, *Resilient Nation*, London, Demos, 2009. http://www.demos.co.uk/files/Resilient_Nation_-_web-1.pdf
[54] Cabinet Office, *Strategic National Framework on Community Resilience*, London, Cabinet Office, 2011, p. 10.
[55] Ibid., p. 4. The definition is drawn from an earlier Cabinet Office resource.
[56] Ibid., p. 5.
[57] David Garland, *The Culture of Control*, Oxford University Press, Oxford, pp.124-127.

"moral" quality, attempting to resonate with a nostalgic vision of (British) community unity in the face of external threat; yet on closer inspection, resilience is posited to be found in rational planning not social bonds: the systematic organisation of the "stiff upper lip".

More briefly, the last example is the Cabinet Office's focus on enhancing "resilient communications". Here, similar to the cyber security example, a major concern is with encouraging industry, emergency services and government to liaise to develop telecommunications systems, and in particular mobile telecoms, better able to provide continuing services in the face of major emergencies. Reflecting on the inability of the then GSM mobile telecommunications to handle the unusually high volume of call and SMS traffic on the day of the London bombings in 2005, a Cabinet Office document urges key users to "[reduce] reliance on GSM mobile communications and [promote] diversity in means of communication"[58]. "Resilient communications" here has a fairly straightforward meaning, though achieving this aim is recognised as a tricky endeavour, requiring technical understanding as to why the GSM system failed, how it cannot be relied on in emergencies, and how both organisational, institutional and technological development would be required to reduce future dependency on the network and create more "resilient" alternatives.

Analysis

Given the high-level role of the Cabinet Office, its co-ordinating function, and many of its particular areas of responsibility, it is perhaps not entirely surprising that the topic of "resilience" is central to many of its policies and activities. The frequency of reference to that term, however, perhaps suggests something further, namely, that the Office regards the term as in many ways encapsulating many of its aims ("enhancing resilience") and areas of responsibility (for example, responding to emergencies). It would seem that for the Office, the way that the term "resilience" can incorporate preventive strategies, emergency planning, contingency strategies, and recovery strategies goes to the heart of what it is tasked to do, and hence is an appealing term to which to refer. Moreover, one can view its activities as part of the delivery of a "resilience" strategy itself – namely, its role in policy development, policy dissemination and helping coordinate the activities of different governmental actors.

This, itself, reveals something interesting about how the Cabinet Office, at least, conceives of the notion of "resilience". First, as is discussed in greater detail above, many of its documents explicitly define or otherwise explain what is meant by the term "resilience" as well as identifying the policy aims in this regard. Secondly, the term is taken to be a "good", in the sense that what is generally urged is "greater" resilience. Third, implicit in the term, and explicit in certain of the subject areas covered, is that the UK may in the future experience significant threats or challenges to everyday life (whether these be natural disasters, pandemics, or security threats), and that these need to be anticipated in a rational manner by central government. However, fourth, while the Cabinet Office clearly has a lead role in improving the UK's "resilience" in various areas, it also recognises that it itself cannot at a stroke implement the desired policies in different areas (and for which, in many cases, other

[58] Civil Contingencies Secretariat, Cabinet Office, *Towards Achieving Resilient Telecommunications: Interim Guidance*, Cabinet Office, undated, p. 3.

government departments are more directly responsible, whether these be in areas such as energy, transport, communications or are delivered at a local level, for example, through regional police forces or are aspects of private sector activities). Instead, for it, the "goal" of "resilience" is best attained through its bureaucratic-rational development, dissemination and co-ordination of coherent multi-agency strategy. Fifth, the notion of "resilience" is used almost exclusively in relation to posited security, health, disaster or other threats; it is not used in relation to "resilience" to or against challenges to democratic society that might be posed by surveillance or security measures, for example. This is perhaps unsurprising, and somewhat obvious, but is worth mentioning simply to note that "resilience" here implicitly supports what might be termed a "pro-security" perspective, even if this is frequently a measured one. Lastly, "resilience" implicitly posits the inevitability of some future threats: only certain threats can be prevented; the rest must be endured, albeit with the benefit of the preparatory damage-limitation measures and infrastructures that the strategy promotes, thereby increasing the likelihood of national survival or community persistence.

Analysis from the IRISS perspective (lessons for resilience strategy)

From the IRISS point of view, some lessons to be learnt are:

- Not uniquely in this case, "resilience" is sometimes undefined but refers to a coherent set of objectives and measures aimed at achieving them in the face of typical human and natural threats to national security and community disruption.
- The resilience strategy relies upon planned, coordinated efforts across organisations at different levels of a national system, and among participants with defined roles and responsibilities.
- The term "resilience" appears to enjoy a certain *political* appeal in the UK today, possibly because the term suggests strength, robustness and fortitude.
- The term "resilience" is also attractive to the *civil service*, perhaps because increasing resilience in practice involves conducting problem analysis, strategic planning, and policy adherence – all of which are consistent with civil service philosophy, especially at a senior level.

2.1.3 Resilience in [dictatorial and] post-dictatorial regimes

Dr Ivan Szekely, Eotvos Karoly Policy Institute

Numerous countries in the world can be considered as post-dictatorial societies in some sense. Even countries with the longest record of democratic rule-of-law traditions have suffered from wars, revolutions, martial law during their history, and these periods resulted in introducing authoritarian leadership, suspending of rights and liberties, and other measures. All these periods in the collective memory of society have had an impact on the *longue durée* characteristics of a population, and on the social and political traditions of a country. In this section, however, we will focus, in geographical terms, on European countries, in temporal terms, on those countries where dictatorial political systems existed after World War II (WWII). From this

group of European countries, we will analyse primarily the post-Soviet societies and, to a lesser extent, societies of certain South-European countries.

Dictatorship itself is a broad concept: a wide range of centralised, authoritarian political systems are understood as some forms of dictatorships. What makes its existence evident is the supreme power of a single ruler and his or her personality cult. However, single-party political systems, centralised administrations supported by strong police forces and secret services, optionally military governance and, above all, restrictions on civil liberties and the institutions of the rule of law are also fundamental elements of a dictatorship. There are authoritarian political regimes, however, which cannot be regarded as dictatorships in the strict sense of the word, even if they have a centralised, single-party leadership and if civil liberties are restricted. China, for example, is a single-party state with an authoritarian political leadership, where practical enforcement of human rights is limited according to western standards, even if it has a market economy based on capitalist principles that govern production, consumption and commerce.

The former societal systems of the countries in our focus, the new European democracies, were not identical either. On the one hand, the history of these countries during the Soviet rule can be divided into characteristic periods, which were induced by changes in the internal political system of the Soviet Union and the individually achieved room for manoeuvring of the leaders of the satellite state. On the other hand, there were significant differences among the political and ideological modalities themselves, which were represented by leaders of the respective countries and were influenced by traditions of the countries concerned. Although large-scale western historiography is sometimes tempted to regard the countries of the "Soviet Bloc" as a homogenous political and social unit, more sophisticated analyses lay stress on important differences among these countries, both before and during the period of communist regimes.

Naturally, there were and are common characteristics in these societies. However, considering the *longue durée* nature of collective mind and certain cultural patterns, post-dictatorial characteristics cannot be understood without understanding the characteristics of the dictatorial periods. Similarly important is to analyse the transition period, the transformation of the political system. We will concentrate on the dichotomy of the political regime and society, from the aspect of resilience of the society towards the dictatorial system, also discussing the resilience of certain dictatorial systems themselves towards political and societal changes, and towards the political and economic pressure of the international community.

The resilience of dictatorial regimes

These characteristics can be best studied in countries of Central and Eastern Europe, which became part of the Soviet sphere of influence during or after WWII but did not become part of the Soviet Union.[59] These countries had to suffer several fundamental changes in their political system during the 20th century. Both individual citizens and their groups, as well as institutions of these countries, developed an ability of resilience towards these changes at various levels. Retrospectively, one may wonder

[59] Albania, Bulgaria, Czechoslovakia, East Germany, Hungary, Poland, Romania, Yugoslavia.

how these Soviet type regimes could remain in power for long decades with their inefficient economies, limited collective and individual freedoms, and low standard of living. First, we need to study whether these regimes themselves were resilient at all towards change and, if yes, which were the main elements of such resilience. The scope of this section does not allow us to analyse this question in great detail; however, we can identify some important factors.

At the international level, the main pillar of these regimes was the political leadership of the Soviet Union, which was always at hand when it was necessary to refer to it in the arena of domestic political infighting, and when the national regimes were required to follow its changes obediently. In turn, when national regimes needed to defend their own standpoints or domestic developments against the Soviet Union or the community of satellite states, they could refer to local public opinion or historical and societal differences.[60] Thus, the room for manoeuvring of the national regimes, including the introduction of drastic measures, was defined by these two poles, the external and internal forces.

The role of the West in the resilience capability of the Soviet-type European regimes is not negligible either. The formal and implicit acceptance of the status quo in Europe not only meant the approval of the actual borderlines of political and military spheres of interest, but, by signing the Helsinki Accords in 1975, it cemented the political division of Europe, too, for the long run (although, paradoxically, this very act started the legitimation process of the demands of dissidents and liberal movements in countries of the Soviet Bloc[61]). Even in moments when a communist regime started to weaken or collapse – as seen best in the case of the 1956 revolution – western political forces, despite exaggerated expectations, did not consider intervening at all.[62] Moreover, when in the late 1980s, the political regimes in the whole region lost their stability, certain western politicians argued against the changing of the status quo in their confidential communications. (Extremely sensitive examples of this approach are the documents of secret negotiations between western and Soviet political leaders in 1989, which have recently become accessible for the broader audience; see, for example, the conversation between Mikhail Gorbachev and Margaret Thatcher.[63]) In the economic sector, the West was willing to finance the indebted economies of countries of the Soviet Bloc by providing loans, and this practice had been significantly contributing to the economic resilience of these regimes.

---

[60] It is important to note that two countries, Yugoslavia and Romania, had developed a partly independent regime, in the case of Yugoslavia the "independent socialist system", while Romania – together with Albania – did not participate in the 1968 invasion of Czechoslovakia, the joint military action of the Soviet satellite states (the members of the Warsaw Pact). Nevertheless, these countries, too, kept following the basic elements of communist ideology.

[61] Mink, Andras, *The Defendant: the State. The Story of the Hungarian Helsinki Committee,* Hungarian Helsinki Committee, Budapest, 2005.

[62] When the National Security Archive, an independent non-profit organisation fighting for open government, managed to have the daily briefings and weekly summaries prepared by the United States Central Intelligence Agency (CIA) declassified as a result of its repeated efforts in the period 2001-2005, it turned out that the events of the revolution did not even reach the level of visibility for the leaders of the CIA. See http://w3.osaarchivum.org/digitalarchive/nsa/index.html

[63] Document No. 85: Record of Conversation between Mikhail Gorbachev and Margaret Thatcher, 23 September 1989, in Svetlana Savranskaya, Thomas Blanton and Vladislav Zubok (eds.), *Masterpieces of History: The Peaceful End of the Cold War in Europe 1989,* Central European University Press, Budapest, New York, 2010.

At the level of internal affairs, the political leadership of the countries of the Soviet Bloc stabilised the regime not only by applying police forces or secret services but also by offering advantages to the new political elite, introducing a number of measures for improving the life standard of important segments of the population, and creating the three-level system of "banning, tolerating, supporting" in cultural politics for intellectuals. Naturally, those publications and artworks belonged to the "supported" category, which reflected the ideology of the political leadership; however, a number of "western-oriented" or "bourgeois" works were also "tolerated", if they did not directly call for actions against the regime. As Janos Kadar, Hungary's communist leader from 1956 to 1988, declared at the beginning of the detente of the political terror following the crushed 1956 revolution, "Who is not against us is with us".[64] The "banned" category was populated by works of internal dissidents, underground art groups and the samizdat[65] publications. However, even in the latter category, certain elements of tolerance could be observed: members of the unofficial opposition were vexed but the operation of their groups was not made completely impossible. In Poland, for example, samizdat editorial activity (which extended to publishing all kinds of cultural or political products which were not available in the official publishers' portfolio, including pornography or esoteric literature) was so wide-spread that during the 1980s, it became an important component of the grey economy. An interesting illustration: the opposition Solidarity movement in Poland (Solidarnost) had its own underground postal stamps printed,[66] which were sold through unofficial channels; the Polish Postal Service was implicitly willing to accept these stamps and deliver the mailings so stamped.[67] Samizdat publications were read not only by members or supporters of the underground opposition, but also by members of the ruling political regime, and this implicit symbiosis contributed to the resilience of the system.

A further interesting strategy of these Soviet type regimes was that it implicitly modified the meaning of generally used notions and expressions having ideological significance, to prevent their direct comparability with the same notions and expressions as used in western democracies. Socialism was the political system these communist-led countries had developed (and not the Swedish model, for example). For them, democracy meant "democratic centralism", not free elections; human rights were exactly what and how such limited rights were granted in these regimes, and not as they were interpreted in the West. Consequently, the possibility for a meaningful dialogue between people from the two dominant political systems was rather limited. Partly as a result of this strategy, these regimes were successful in creating a positive

[64] Declared at the meeting of the Patriotic People's Front in 1961, in sharp contrast to the statements of the country's authoritarian leader preceding the revolution, Matyas Rakosi, who used to say, "Who is not with us is against us."

[65] Samizdat was a grassroots dissident activity across the Soviet Bloc in which underground publications were created, reproduced or copied, and distributed through unofficial channels. In a broader sense, samizdat is all kinds of self-produced communication forms which are officially banned or censored, such as the early period of the B92 radio station which was operating during the Yugoslavian wars in the 1990s, or the Internet forums of today aimed at circumventing state censorship. See http://www.samizdatportal.org/

[66] It is estimated that in 1986 alone, around 200 sets of stamps were produced in print runs of 5,000-10,000 each.

[67] See Polish Underground Ephemera. http://www.osaarchivum.org/greenfield/repository/osa:554e8ec5-a131-4087-9b5d-4551cc82b291

public opinion on important elements of the political and social system in a significant majority of the population, despite widespread critical opinions and resistance of the citizens towards the regime.[68]

All these characteristics made Soviet-type political regimes able to reduce tensions arising at both international and national levels, to adapt to the changing environments, and to resist shock-like impacts. (Among the latter, during the 1956 Hungarian revolution and the 1968 invasion of Czechoslovakia, military forces were deployed, and the reactions of the regime cannot be regarded as a form a resilience; however, elements of the consolidation periods following these events can again be considered as signs of resilience of the political system.)

All this seems to contradict regime theory, according to which "authoritarian systems are inherently fragile because of weak legitimacy, overreliance on coercion, overcentralisation of decision making, and the predominance of personal power over institutional norms", as referred to by Nathan (2003).[69] Other types of centralised, authoritarian systems may also show a significant ability to adapt to changes and to resist stresses and shocks. As Nathan notes, many western observers thought that after the Tiananmen crisis of 1989, the rule of the Chinese Communist Party would collapse and the country would follow the wave of western-type democratisation. Instead, the regime reconsolidated itself, and China has become a world power with a relatively high level of stability in domestic and international domains.[70]

The resilience of citizens of dictatorial regimes

How did individual citizens become resilient in such regimes? What did they become resilient to? To what extent did they identify themselves with the regime? What techniques did they apply to preserve their individual and group identity, and their personal freedom?

Although it would be a mistake to oversimplify social stratification (and political leadership itself cannot be regarded independent from the social environment either, even in a dictatorial regime), still, the group of those accepting the regime to a certain extent and the group of those strongly opposing it can easily be distinguished. For the acceptants, the direct objective was to retain and to develop family life and personal

[68] A valuable corpus of data and documents of public opinion research became recently available at the OSA Archivum (www.osaarchivum.org), created by a unique institution, the Hungarian Public Opinion Research Institute (formerly Mass Communications Research Center), which had been using western scientific methodology for exploring public thought in Hungary during the communist period, and thus patterns of pre-transition public thoughts have become directly comparable with those in the democratic period (http://osaarchivum.org/db/fa/420.htm). One of the empirical surveys showed that in 1981 the majority of the population was convinced that life conditions including the right to work, the protection of workers' interests, the quality of health services, the general ethical level of society, the freedom of expression etc. were all guaranteed at a higher level in Hungary than in western countries. (The number of those with this opinion, however, had radically decreased by 1987.)

[69] Nathan, A.J., "Authoritarian Resilience", *Journal of Democracy,* Vol. 14, No. 1, 2003, pp. 6-17.

[70] Nathan emphasises four aspects of the Chinese communist regime's institutionalisation and resilience: the increasingly norm-bound nature of its succession politics; the increase in meritocratic as opposed to factional considerations in the promotion of political elites; the differentiation and functional specialisation of institutions within the regime; and the establishment of institutions for political participation and appeal that strengthen the Communist Party's legitimacy among the public at large. Nathan, A.J., "Authoritarian Resilience", *Journal of Democracy,* Vol. 14, No. 1, 2003, pp.6-17.

economy, and this was achieved through exploiting the small-scale semi-private forms of enterprise offered by the more liberal economic systems in the Soviet Bloc (for example, self-employed operation of small restaurants and shops, or auxiliary workshops of co-operatives) and using their informal economic networks.

Those openly opposing the regime – even if they did not belong to the groups applying the toolbox of underground movements, which were able to quickly re-organise themselves after a police raid, but belonged to critical-minded, intellectual circles the members of which were involved in the activities of the opposition, for example, in editing and distributing underground publications – developed a common toolbox of resilience, including joint cultural experiences, sharing of samizdat literature, organising underground intellectual events (such as the lectures of the "Flying University" in Poland and Hungary, an informal series of lectures organised in the flats of members of the opposition), or even developing a self-reflecting irony to ease psychological tension: important information was sometimes spelt ironically into the light switch as if there were a bug in it (and sometimes there was).

The harshness of the dictatorship naturally determined the behaviour of its opposition, its tactics and its resilience, too. In the Soviet Union where the regime took harsh measures against the opposition during the majority of the post-war periods, these measures made the members of the internal emigration more resilient, especially those who received moral and sometimes financial support, partly from each other, partly – through unofficial channels – from their friends in the West.

The place of an individual on the virtual range of accepting or rejecting the political regime can be evaluated from various aspects. In certain cases, the acceptance was only formal: according to the radical judgement of Los, people in communist regimes developed a strong control over their body language in order to produce a uniform appearance and mask their opinion. This could be the case in regimes exerting stronger control over their citizens, especially in periods of increased repression. In other cases, the same intellectuals published their works in the "supported" and the "tolerated" categories, or even in samizdat publications (mostly under pen names), for example, in Poland and Hungary in the 1980s, and this can be regarded as a sort of intellectual symbiosis with the ruling regime.

Both in countries of the Soviet Bloc and in those South-European countries where dictatorial regimes were in power after WWII (in the case of Spain, Portugal and Greece until the mid-1970s), the unequal informational relationship between the governing and the governed, the extensive network of agents reporting on individual citizens, and the wide-spread practice of surveillance were common characteristics of these regimes. The unequal informational relationship included the reality of the transparent citizen vis-à-vis the opaque state, where data, statistics and trends in society were hidden or falsified according to party interests, information was provided in a paternalistic manner and society was governed partly by secret decisions and orders.[71]

[71] Szekely, Ivan, "Central and Eastern Europe: Starting from Scratch", in Ann Florini (ed.), *The Right to Know. Transparency for an Open World,* Columbia University Press, 2007, pp.124-150.

Characteristics of the transition period

The characteristics of the period of the democratic turn and the political transformation can be best observed in countries of the disintegrating Soviet Bloc, since fundamental changes took place in a historically very short period, and were connected with the collapse of a common repressive regime. The notion of resilience is difficult to interpret in a transitional period when the points of reference themselves are on the move. However, from the aspect of state power and the political system, the so-called "velvet revolution" (Czechoslovakia) or "rule-of-law revolution" (Hungary), in other words: yielding the power to the new political leadership through negotiations (the so-called Round Table Talks in several countries of the region in 1989-1990), which retained the legal and administrative framework throughout the whole process, can be regarded as a sort of structural resilience, in contrast to those countries where the collapse of the old regime was accompanied by abolishing laws and institutions, bloodshed or even executions, as was the case in Romania. The biggest advantages of the negotiated transition were the limited extent of social and economic losses, and the fact that there was no period when law, judicature and state administration did not work. Its disadvantages were, however, the smaller or missing catharsis from a social psychological point of view, and the possibilities of newly authoritarian ambitions, the advocates of which may declare the historical period after the transition as illegitimate, and introduce, on this ground, a newly centralised political and ideological regime restricting democratic rights and freedoms.

An interesting form of intertwining of personal and institutional resilience, characteristic to the transition period in countries of the former Soviet Bloc, was how members of the former political and economic elite managed to save their formal and informal influence in the new political system. A favourite procedure was to privatise state-owned companies in a way that these properties could be taken over by their former managers (or their family members or acquaintances) at a very low price, or to occupy strategic positions in the newly privatised companies. There is a strong tradition of resilience in the area of social and political influence spanning over changes of the political system in these countries: in Hungary, for example, members of the far-right, pro-Nazi Arrow Cross Party, who committed grave atrocities before and during WWII, became employed in the infamous communist secret police (AVO, later AVH) in the 1950s, demonstrating that every regime needs uninhibited henchmen; or after the 1989 changes, contrary to expectations, the local elections in the majority of towns and villages resulted in reinforcing the positions of the former leaders of municipal councils as newly elected mayors. There was a popular opinion after the regime change, especially in the countryside, that certain people or families would be leaders in every political system, or would occupy the key positions in any periods (e.g. someone who, before WWII, worked as a steward for a landlord became the leader of an agricultural co-operative during the communist times, and after the political changes of 1989 became a big landowner; similar life stories are evident for veterinarians or apothecaries, etc.).Later, this practice came to an end, due to large scale privatisation, the investments of foreign capital and the foreign management of those companies which became part of multinational holdings. However, a part of the surviving economic positions remained active, and were inherited by the new generations of families.

The legitimacy of the law enforcement agencies, especially the secret police, of the dictatorial regimes collapsed in the period of the political transition, and these organisations suffered a spectacular material and moral loss. The population regarded these organisations – together with the authorities of the dictatorial administrative system – as unprincipled servants of the past regime, while the new political forces regarded these organisations as untrustworthy and thus in need of a radical restructure. After the shock, however, the secret services – much less spectacularly – managed to reconsolidate themselves within a relatively short period. Although the leaders of these organisations in most countries of the Central and Eastern European region were replaced with trustworthy people committed to the new democratic regime, a significant part of the personnel remained in office, together with their organisational culture, and adapted to the changing environment. Every regime, including democratic constitutional states, need secret services and the related expertise, thus this consolidation was also in the interest of the new regimes. An important element of the resilience of the secret services has been that although the heads of these organisations are always appointed by the actual political regime, their internal working system and their work ethos are rather autonomous.

Wiretapping scandals got high publicity in countries of the Central and Eastern European region during the period of political changes (the best-known among these was the so-called Hungarian Watergate, or Duna-gate scandal, which revealed that during the democratic turn, Hungarian secret services were keeping the leaders of the new political forces under surveillance) and this further eroded the legitimacy of the secret services. Still, the establishment of the new, legitimate secret services took place quickly, and the new organisations – challenging legislative and public pressure alike – managed to share among themselves a significant part of the documentary heritage of their former organisations and were (and still are) using these documents during their activities in the democratic period, too.

Forms of resilience in the post-dictatorial period

Among the newly democratic countries, the range of mobility and the level of autonomy significantly increased, both for participants of the political system and for members of the society. This was due not only to the newly granted possibilities (establishing civil and political organisations, organised representation of interests, practical enforceability of individual rights and freedoms, capitalist economic environment, etc.) but also to the fact that, in line with the decomposition or transformation of the old legal and administrative framework, a unique window of opportunity emerged for establishing new institutions and new international relationships, both at individual and organisational levels. Such opportunities were much more limited later, in the consolidation period of the new regimes and after the initial euphoria in public opinion. If actors of a certain domain were able to use this historical window of opportunity for establishing their legal and institutional framework and laying down the fundamentals of a rule-of-law system (to an extent that would have not been possible later, in a much less favourable political environment), this resulted in an increased level of a specific institutional-legal form of resilience for the longer run.[72] Countries where the newly democratic governments

[72] This can be observed in Hungary in the history of the independent supervisory authority in the area of informational rights (the Parliamentary Commissioner for Data Protection and Freedom of Information), as well as the related legislation: the permeating of the Hungarian legal corpus by

missed the opportunity to establish these fundamentals – saying that they would leave them until popular demand arises – could never fully reach the level of early reacting countries in these areas.

All this could lead us to conclude that, in parallel with the increasing possibilities and enhancing autonomy, the resilience of all social strata has become stronger towards adverse impacts, as compared to the dictatorial period. However, experience does not fully support this assumption; recent history shows that a number of democratic political organisations established without historical experience proved to be vulnerable and short-lived. Interest-representing organisations such as trade unions became marginalised due to the far-sightedness of experienced foreign investors. Certain social groups, mainly the unskilled and the intellectuals, started to lose their positions and were able to retain their life standards only through great difficulties. At the individual level, for members of the older generations, who had been living and working during the past regime, too, preserving their identity, re-evaluating their personal past often caused psychological difficulties or traumas.

Recent research,[73] which compared the patterns and strength of intellectuals' personal networks in Hungary in 1988 and in 2005, led to the somewhat surprising result that a majority of the intellectuals today have no more, or have even fewer usable contacts than they had in 1988, so in the case of adverse situations, they have fewer opportunities to mobilise these contacts – in other words, their resilience may have decreased. This research result indicates that in the environment of a stable, although dictatorial, regime, it was easier to build up a workable network of personal relationships for the intellectuals than in a changing milieu.

The formation of resilience of society towards surveillance in the post-dictatorial societies also deserves attention. According to Los, one of the factors of the long-lasting impact of dictatorial surveillance in these societies is the "conversion of fear": after the political changes, the fear of the repressive regime was soon replaced by a fear of crime.[74] Another conclusion by Los is that societies under long authoritarian rule in the 20th century virtually skipped the period of democratic modernity and jumped directly into the surveillance culture of postmodernity. The lack of historical experience resulted in an increased level of vulnerability of members of these societies, and a decreased level of resilience towards new forms and technologies of surveillance. As Szekely observed, members of these societies are less experienced and more gullible vis-à-vis business and marketing offers, including industry-driven surveillance.[75]

In the former dictatorial regimes where personal and family life were more resilient towards the political system (in other words, people's vigilance, their strategies and

---

provisions on processing of personal data, and the quasi case law of the Commissioner, became durable elements of the newly democratic regime – even if the present political forces have restricted these informational rights, dismissed the Commissioner in office prematurely, closed down the institution and replaced it with a government authority.

[73] See Kmetty, Zoltán, "Networks, resources, interactions", paper presented at the conference *"TK 3.0: Did People Lie in Kádár's Hungary?"* OSA Archivum, 29 April 2013.

[74] Los, Maria, "Post-communist fear of crime and the commercialization of security", *Theoretical Criminology*, Vol. 6, No. 2, 2002.

[75] Szekely, Ivan, "Hungary", in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation,* Edward Elgar Publishing Ltd., November 2008.

tactics were concentrated against the institutions of political power, for example, the secret police), while private surveillance was not conceived as potentially harmful, the suspicion against state surveillance remained high. New forms of business-driven surveillance met a conspicuous apathy – this is what Samatas calls "the Greek surveillance paradox".[76]

2.1.4 Resilience in the US: cyber security and critical infrastructure protection

Dr Rocco Bellanova, Peace Research Institute of Oslo

The choice of relevant documents

For our analysis of the use of the term *resilience* by United States' (US) institutions, we concentrate on strategic and policy-oriented documents concerning national and homeland security.[77] While the official use of the term *resilience* is surely not limited to the fields of security, critical infrastructure protection and cyber-security, these areas are extremely relevant for the IRISS project and its focus on surveillance. Indeed, many of the strategic documents in these fields propose policies that foster, implicitly or explicitly, surveillance measures. All the selected documents have been published between 2002 and February 2013. This timeframe of reference is particularly pertinent because it covers a series of major policy decisions, from the creation of the Department of Homeland Security (DHS) in 2002 and the release of the first National Security Strategy of former President G.W. Bush, to the adoption of a Presidential Policy Directive on Critical Infrastructure Security and Resilience in February 2013. In both our selection and analysis, we have favoured the most high-level documents, especially national and international strategies. As the National Security and Homeland Security strategies are a sort of periodic documents, one of the advantages of focusing on them is to highlight trends and eventual shifts in the official discourse and the agenda-setting. The remaining documents are more sector-specific (critical infrastructure protection and cyber-security), and they can provide precious material to better understand specific, applied uses of resilience.

Explicit definition(s)

Despite wide use of the term – discussed in the section below in more detail – the analysis of the documents supports the impression that resilience remains a rather under-defined notion. The most extensive definition is provided in the Presidential Policy Directive - Critical Infrastructure Security and Resilience:

> The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to

[76] Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in William C. Webster, Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2,* Editura Universităţii "Alexandru Ioan Cuza", Iasi, 2011.

[77] The full list of documents is provided at the end of this section. We mostly focused on texts published by the White House and the Department of Homeland Security.

> withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.[78]

The above definition seems elaborated on the base of that already introduced in the 2010 National Security Strategy. In the National Security Strategy, resilience is defined as "the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption".[79]

A very similar definition is also proposed in the Glossary of the Office of Infrastructure Protection Strategic Plan: "Resilience: ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions".[80] This definition introduces two quite interesting differences: the first concerns the introduction of the adverb "successfully", and the second the pairing of a somehow more neutral "change in conditions" to "adversity" (instead of disruptions, attacks, accidents, incidents or threats). These small differences open the idea of resilience not only as mere bouncing back or survival, but also as an occasion to grow stronger after adversity.

The 2007 National Strategy for Homeland Security identifies two main types of resilience: "structural" and "operational".[81] Structural resilience is defined as the "the ability of power, communications, and other life sustaining systems to survive an attack by terrorists, a natural disaster, and other assessed risks or hazards".[82] The definition of operational resilience is even more interesting, as it considers the government itself a sort of critical infrastructure

> to maintain comprehensive and effective continuity programs, including those that integrate continuity of operations and continuity of government programs, to ensure the preservation of our government under the Constitution and the continuing performance of national essential functions – those government roles that are necessary to lead and sustain the Nation during and following a catastrophic emergency.[83]

The 2009 Cyberspace Policy Review does not provide an explicit definition of resilience, but a short summary of the main requirements to achieve cyberspace "resiliency":

> [t]he infrastructure must be resilient against physical damage, unauthorized manipulation, and electronic assault. In addition to protection of the information itself, a risk mitigation strategy for cyberspace must focus on the devices used to access the infrastructure, the services provided by the infrastructure, supporting elements of the networks, and all means of moving, storing, and processing information. The strategy also must include prevention, mitigation, and response against threats to or subversion of the people who operate and benefit from the infrastructure, the processes that run or

[78] The White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience", The White House, Washington, DC, 2013.
[79] The White House, "National Security Strategy", The White House, Washington, DC, 2010, p.18.
[80] Office of Infrastructure Protection, "Office of Infrastructure Protection Strategic Plan: 2012-2016", Department of Homeland Security, Washington, DC, 2012, pp.14, emphasis in original
[81] Homeland Security Council, "National Strategy for Homeland Security", The White House, Washington, DC, 2007.
[82] Ibid., p. 28.
[83] Ibid., p. 29.

> take advantage of the infrastructure, and the supply chains used to build and maintain the infrastructure.[84]

A growing and generalised use of the word resilience

The first insight drawn from a text analysis of this set of documents is that the use of the word resilience has not only grown, but has also been generalised. This is particularly evident in the national and homeland security strategies. In the 2002 National Security Strategy the term *resilien** only occurs once, at the very end of the document, where it refers to the "resilience of [US] institutions" among the sources of "America strength".[85] The 2006 National Security Strategy does not mention the term at all.[86] However, resilience becomes a key term of the 2010 National Security Strategy, where not only a full sub-chapter is dedicated to the "strengthen [of] security and resilience at home",[87] but the resilience of "citizens, communities, and economy" is considered an important element of national security itself.[88]

Resilience is conceived as a feature, or better a strength that is already present, that is more or less latent, and more or less accounted for in institutional practices. Still, this strength deserves further attention and nurturing. It is also interesting to note that the adjective resilient is often used to describe the "nation" and the "homeland", both to portray them as they currently are, and to explain how they should be. The national or homeland resilience is not the mere result of the action of federal government, but of the fostering (by the government) of the somehow innate character of Americans (private citizens or private companies). One passage of the 2010 National Security Strategy is particularly telling:

> The ideas, values, energy, creativity, and resilience of our citizens are America's greatest resource. We will support the development of prepared, vigilant, and engaged communities and underscore that our citizens are the heart of a resilient country.[89]

This diffuse and strategic use of the term resilience mirrors a rather generic definition of what resilience means. A definition is provided (cf. section above), but only few concrete elements are advanced in specific cases, as if resilience was a sort of self-explaining term. Finally, it is noteworthy that the societal dimension of resilience is practically absent when it comes to cyberspace. In this case, the resilience sought to be achieved is that of (information) "networks" and "critical government and industry systems and networks".[90]

A similar trend towards an increased and diffuse use of the term *resilien** can be highlighted in the strategic documents concerning Homeland Security. The first National Strategy for Homeland Security, released in 2002, does not use at all the

---

[84] The White House, "Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure", The White House, Washington, DC, 2009, p. 31.
[85] The White House, "The National Security Strategy of the United States of America", The White House, Washington, DC, 2002, p. 31.
[86] The White House, The National Security Strategy of the United States of America", The White House, Washington, DC, 2006.
[87] The White House, "National Security Strategy", 2010, pp.18-19.
[88] Ibid., p. 10.
[89] Ibid., p. 16
[90] Ibid., p. 27

term.[91] Still, few years later, when the second National Strategy for Homeland Security was published in 2007, both the "resilience" and "resilient" appear frequently, especially regarding critical infrastructure protection.[92] In the 2007 Homeland Security strategy it is the protection of critical infrastructure and key assets that permits to "build […] a more resilient Nation".[93] The same document also introduces the notion of "operational resilience" (cf. above), which refers to the ability to ensure organisational continuity in case of disaster.[94] The 2010 National Security Strategy sees the achievement of a resilient nation as based on the recognition and nurturing of a resilient society (and economy).

The firm adoption of the term *resilien** in the Homeland Security jargon seems further confirmed by its even wider use in the 2012 US Department of Homeland Security Strategic Plan[95] which defines the mission, vision and goals of the department for 2012-2016. This text generalises the term "resilience": not only is it used in relation to critical infrastructure protection,[96] it is also used in relation to the "nation" and "homeland", and in particular to "disasters".[97] Indeed, an entire "mission" is dedicated to ensuring resilience to disasters, aimed at mitigating hazards, enhancing national preparedness through a community approach to emergency management, ensuring effective emergency response, and rapidly recovering from a catastrophic event.

The same document proposes a list of "performance measures", prompting the collection of statistical data, as well as setting targets to be met each year, on factors such as "households surveyed reporting they have taken steps to be prepared in the event of a disaster", or "urban search and rescue teams arriving on scene within 12 hours of deployment notification".[98] Finally, the term is also used in relation to cyberspace, but only with reference to the "software that enables and controls systems and networks".[99]

In addition to the main strategic documents for national and homeland security, some complementary documents concerning critical infrastructure protection and cyber-security are particularly telling. In these texts, the term *resilien** is present from the first publications, i.e., the National Strategy for The Physical Protection of Critical Infrastructures and Key Assets[100] and the National Strategy to Secure Cyberspace,[101]

---

[91] Office of Homeland Security, "National Strategy for Homeland Security", The White House, Washington, DC, 2002.
[92] Homeland Security Council, 2007.
[93] "By protecting CI/KR, we further protect the American people and build a safer, more secure, and more resilient Nation"; Ibid., p. 25
[94] Ibid., p. 29
[95] Department of Homeland Security, "Department of Homeland Security Strategic Plan. Fiscal Years 2012-2016", Department of Homeland Security, Washington, DC, 2012.
[96] Cf. "Objective 1.3.3: Make critical infrastructure resilient"; ibid., p. 5
[97] For example, the main mission of the DHS is defined as follows: "We will lead efforts to achieve a safe, secure, and **resilient homeland**. We will counter terrorism and enhance our security; secure and manage our borders; enforce and administer our immigration laws; protect cyber networks and critical infrastructure; and ensure **resilience from disasters**"; [Department of Homeland Security, 2012 #10@ 2, emphasis added]
[98] Department of Homeland Security, 2012, p. 18.
[99] Ibid., p. 12.
[100] The White House, "The National Strategy for The Physical Protection of Critical Infrastrctures and Key Assets", The White House, Washington, DC, 2003.

both released in February 2003. The documents concerning critical infrastructure protection make more use of the term resilience, in particular when it comes to strategic plans. For example, the 2009 National Infrastructure Protection Plan[102] employs both the word and the adjective frequently (128 times in 176 pages) and the 2012 Office of Infrastructure Protection Strategic Plan[103] uses it nearly every page (41 occurrences in 16 pages). This trend seems further reinforced by the phrasing of the 2013 Presidential Policy Directive on Critical Infrastructure Security and Resilience, which is one of the few documents that proposes an explicit definition of the term (cf. section above).[104]

In cyber-security, the trend on the use of the term 'resilience' is less evident. As mentioned above, the word has been used since 2003, and is used in all the other documents collected. Resilience, or better: "Assuring a Trusted and Resilient Information and Communications Infrastructure", is clearly stated as the main purpose of the Cyberspace Policy Review of 2009,[105] but the accompanying document presenting "The Comprehensive National Cybersecurity Initiative" of President Obama merely mentions "resiliency" in the concluding lines.[106] The term *resilien** is again used in the International Strategy for Cyberspace, but not with the same emphasis and frequency of the documents concerning critical infrastructure protection and national security.[107] Finally, in the 2013 Executive Order on Improving Critical Infrastructure Cybersecurity, the term is used only once, as a guiding policy goal.[108] All these documents mention resilience in relation to the infrastructures, the networks or the information systems, and often as a condition that is not yet fully achieved. From this point of view, the very premise of the 2009 Cyberspace Policy Review is very programmatic:

> The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations.[109]

---

[101] The White House, "The National Strategy to Secure Cyberspace", The White House, Washington, DC, 2003.
[102] Department of Homeland Security, "National Infrastructure Protection Plan", Department of Homeland Security, Washington, DC, 2009.
[103] Office of Infrastructure Protection, 2012.
[104] The White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience", 2013.
[105] The White House, "Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009.
[106] The White House, Press Office, "The Comprehensive National Cybersecurity Initiative", The White House, Washington, DC, 2009..
[107] The White House, "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", The White House, Washington, DC, 2011.
[108] "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"; The White House, "Executive Order -- Improving Critical Infrastructure Cybersecurity", The White House, Washington, DC, 2013.
[109] The White House, "Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009, p. i.

The multiplication of the referent objects of resilience

As already mentioned above, the documents selected for reference in this section not only highlight a growing "statistical" use of the term, but also its generalisation. This is in fact a sort of double generalisation. The first step is the move from the sector specific documents concerning critical infrastructure protection and cyber-security to those that have an overall strategic scope, i.e. the national and homeland security strategies. This first step is particularly evident in the two national strategies for homeland security: while in 2002 there is no use of the term, in the 2007 strategy, the term is introduced and mostly used in a chapter dedicated to the "mitigation" of "vulnerabilities" of critical infrastructure and key resources (including cyber-security).[110]

The second step in the generalisation is the diffusion of the term beyond critical infrastructure protection. This is evident in the 2010 National Security Strategy, where it is stated, inter alia, that "national security draws on the strength and resilience of our citizens, communities, and economy".[111] The multiplication of the referent objects of resilience is confirmed in the DHS Strategic Plan for the period 2012-2016. In this document, resilience not only refers to material infrastructures or information systems, but also that of "global movement systems", "key nodes of transaction and exchange within the global supply chain", "maritime transportation systems", "communities", indeed, the entire "Nation".[112]

We can detect an important trend in this second step of the generalisation: a re-orientation of the capacities of resilience, or of their enhancement, towards the constitution of a "resilient nation". Then, each form, each practice, each strategy of resilience should be aimed, more or less explicitly, at reinforcing the resilience of the 'total', and not only at merely surviving a specific shock or disruption. From this perspective, while this diffusion and generalisation of the term recognise the agency of many different actors, they also introduce an attempt to institutionalise resilience.

The rationales and the justifications for resilience

This double generalisation of the term 'resilience' is grounded on the cumulation of intertwined rationales: limiting cascade consequences; acknowledging the possible occurrence of disruptions; stimulating and rallying a wide and diverse group of actors.

In first instance, the main justification to foster resilience is that of mitigating the vulnerabilities of systems the eventual failure of which could engender severe cascade consequences. This justification is premised on the idea that some infrastructures are the backbone of modern societies, and their disruption would have far-reaching effects because of their interconnectedness and their key role in everyday life. For example, the 2007 National Strategy for Homeland Security states that

> [a] failure in one area, such as our water supply system, can adversely affect not only public health but also the ability of first responders to provide emergency services.

[110] Homeland Security Council, 2007, pp. 27-30.
[111] The White House, "National Security Strategy", 2010, p. 10.
[112] Department of Homeland Security, "Department of Homeland Security Strategic Plan. Fiscal Years 2012-2016", 2012.

> Accordingly, ensuring the survivability of our CI/KR [critical infrastructures/key resources] assets, systems, and networks requires that we continue to accurately model their interdependencies and better assess and understand the potential cascading effects that could impact and impede operations in interconnected infrastructures.[113]

This rationale pushes the resilience of critical infrastructure in the main strategic agenda, and thus mirrors the first step of the generalisation of the term.

The second rationale to promote resilience is the explicit acknowledgement, by the federal government, of the impossibility to prevent and avoid all disruptions. The premise is that "100% security" is not an achievable goal, and it is not something that can be promised or assured, not even in the best conditions, as there are too many different potential sources of disruptions that cannot be fully controlled. In this sense, the 2010 National Security Strategy states that

> at home, the United States is pursuing a strategy capable of meeting the full range of threats and hazards to our communities. These threats and hazards include terrorism, natural disasters, large-scale cyber attacks, and pandemics. As we do everything within our power to prevent these dangers, we also recognize that we will not be able to deter or prevent every single threat. That is why we must also enhance our resilience.[114]

Therefore, the strategic response is that resilience should not be limited to infrastructures, but should also be recognised and nurtured in regards to other core elements of the "homeland" or of the entire "nation". This move mirrors the second step of the generalisation of the term: the multiplication of referent objects.

Furthermore, these two rationales are intertwined with a third one: resilience implies a rallying together of a wider group of actors, sharing both forces and responsibilities for the (continuous) preparation against adverse events and the punctual mobilisation in case of disruption. For example, the 2010 National Security Strategy states

> [t]he private sector, which owns and operates most of the nation's critical infrastructure, plays a vital role in preparing for and recovering from disasters. We must, therefore, strengthen public-private partnerships... We will emphasize individual and community preparedness and resilience through frequent engagement that provides clear and reliable risk and emergency information to the public. A key part of this effort is providing practical steps that all Americans can take to protect themselves, their families, and their neighbors.[115]

Again, this rationale is somehow cumulative to the other two. The premises are that infrastructures are largely owned and operated by private actors and these actors have a better expertise. Moreover, non-governmental actors, such as communities, have their own latent strengths and they show these forces in time of distress. Finally, the US has a tradition of limited intervention by the federal government, and it rather favours the intervention of the more local institutions. By focusing on resilience, the panorama *in* which the federal government should act, as well as the panorama *on* which it should act, is partially redefined. An increasing number of diverse actors, their latent strengths, their specific knowledge and competences, should be accounted,

[113] Homeland Security Council, 2007, pp. 27-28.
[114] The White House, "National Security Strategy", 2010, p. 18.
[115] Ibid., p. 19.

in the double sense of taken into consideration (and praised), but also measured and fostered. This rationality of mustering diverse actors mirrors the increasing trend that we have detected in the use of the term: the attempted institutionalisation of resilience.

These three rationalities are largely intertwined and, together, they could describe resilience as a specific rationality of governing. Indeed, it is the very role of the federal government that seems re-thought: on the one side, less direct engagement in what have been recognised core but fragile nodes (e.g., critical infrastructures). On the other side, there is an attempt to control forces and fields where there was only little expertise or involvement (e.g., cyberspace, but also communities). In both cases, the privileged tools are the collection of statistics, the definition of goals and targets, and the creation of private-public partnerships.

Distillation of the features of elements of resilience

Some core elements emerge from the analysis of the main documents and from the identification of the main definitions. These include:

- the ability to identify and mitigate vulnerabilities;
- the acknowledgement of the complexity of systems and the reliance of societal activities on them;
- the acknowledgement of the impossibility to ensure maximal security, and the need to accept risk(s);
- the need to foresee and prepare against disruptions;
- the need to rally different and new actors, sharing responsibilities, knowledge and resources with them;
- a certain level of institutionalisation of the latent strengths, nurture and train and share responsibilities with relevant stakeholders.

Policy tools

As evident in the analysis of the set of documents, the fields of intervention are increasing with the generalisation of the use of the term “resilience”. From critical infrastructure protection to disaster prevention, from cyberspace to economic security, achieving and fostering resilience is among the policy priorities set in strategic documents.

Several policy tools can be employed in the development of a resilience strategy. A crucial policy tool is the formulation of comprehensive strategic plans, with specific goals and objectives. Public-private partnerships might help in resilience strategies. A risk-management approach will help identify threats, vulnerabilities and the best solutions to reduce the consequences of disruption. Redundant systems and technological innovation can also form part of a resilience strategy.

Analysis from an IRISS perspective

With respect to the general purposes of the IRISS project, and the analysis of the chosen set of documents, we advance some general comments.

In none of the documents reviewed for this section, is resilience considered a possible response to surveillance. It is not even taken into consideration as a desirable substitute to the increase of state-run or supported surveillance. On the contrary, the resilience of the communities is perceived as a further potential layer of surveillance (e.g., in the program of the kind "if you see something, say something") to be added to what is already proposed by government authorities.

All documents mention the possibility of resilience of institutions (e.g., the Congress, the courts, national governments, etc.) or of the media to counter either government or private sector forms of surveillance. The resilience of institutions is conceived as "operational resilience", mentioned in the 2007 National Strategy for Homeland Security, which refers to the capacity of institutions to keep the lead of operations in case of disruption.

The "language" of resilience permits one to identify and include a series of diverse actors that were previously taken into little consideration in the field of (national) security. However, when it comes to societal actors, they are enlisted as either private actors (companies and business) or communities. Practically nothing is said about individuals or about different and diverging forms of collectivities. Nevertheless, it is reasonable to think that these 'side-lined' actors are important in terms of resilience to surveillance.

The engagement of societal actors tends to be a specific way to institutionalise resilience and their relative latent strengths. To some extent, this is a way to tame and take advantage of the unexpected and of the non-easily accountable. To this purpose, one important tool is the creation of plans and the definition of performance measures.

On no occasion is the reinforced role of private companies assessed in terms of potential negative effects on society and individuals, e.g., the possible negative consequences of reinforced private surveillance in the workplace of critical infrastructures.

In the case of cyber-security, resilience is mostly seen in terms of the resilience of information systems, of networks and hardware. In this specific case, resilience is an opportunity for a government to enter a domain in which it is not considered the most important player.

The ambiguity of the definition of resilience is most probably what permits its diffuse use in different jargons and with different referent objects. While this leaves a certain margin of manoeuvre to the institutions, it also risks emptying the term of any possible specific meaning or specific re-appropriation by non-institutional actors.

The increasing emphasis on the need to build a "resilient nation", where the different forms and practices of resilience (of diverse actors) should converge, risks obliterating the political potentialities of resilience. Within this horizon, the possibility of specific resilient practices to question the choices of the government (e.g., in terms of surveillance) is somehow downplayed. Furthermore, the role of the federal government to co-ordinate, supervise and nurture resilience can pave the way to the deployment of further surveillance measures.

Notwithstanding the generalisation of the use of the term, the reference to the resilience of material infrastructures remains current. These non-human and non-institutional elements are important even in the more strategic and policy-oriented documents, and particular attention is devoted to their design and their web of interactions. Still, no questioning of the state of play of these relations and entanglements (political, economic and societal) is advanced: no radical alternative is proposed, only marginal adjustments.

References

Department of Homeland Security, "National Infrastructure Protection Plan", Department of Homeland Security, Washington, DC, 2009.

Department of Homeland Security, "Department of Homeland Security Strategic Plan. Fiscal Years 2012-2016", Department of Homeland Security, Washington, DC, 2012.

Homeland Security Council, "National Strategy for Homeland Security", The White House, Washington, DC, 2007.

Office of Homeland Security, "National Strategy for Homeland Security", The White House, Washington, DC, 2002.

Office of Infrastructure Protection, "Office of Infrastructure Protection Strategic Plan: 2012-2016", Department of Homeland Security, Washington, DC, 2012.

The White House, "The National Security Strategy of the United States of America", The White House, Washington, DC, 2002.

The White House, "The National Strategy for The Physical Protection of Critical Infrastrctures and Key Assets", The White House, Washington, DC, 2003.

The White House, "The National Strategy to Secure Cyberspace", The White House, Washington, DC, 2003.

The White House, "The National Security Strategy of the United States of America", The White House, Washington, DC, 2006.

The White House, "Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure", The White House, Washington, DC, 2009.

The White House, "National Security Strategy", The White House, Washington, DC, 2010.

The White House, "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", The White House, Washington, DC, 2011.

The White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience", The White House, Washington, DC, 2013.

The White House, "Executive Order -- Improving Critical Infrastructure Cybersecurity", The White House, Washington, DC, 2013.

The White House, Press Office, "The Comprehensive National Cybersecurity Initiative", The White House, Washington, DC, 2009.

2.1.5 The UN and resilience

Professor Charles Raab and Dr Richard Jones, University of Edinburgh

The terms "resilience" and "resilient" are used profusely as normative and empirical language in many United Nations (UN) documents, although in others their relevance and meaning are matters of inference and interpretation. The UN's ramified institutional structure, vast diversity of fields of interest and multiplicity of special reports by panels and task forces give rise, in some fields, to ubiquitous reference to resilience as a desirable aim or as a property of some natural or human process. To be resilient is regarded as desirable; becoming resilient is regarded as an important policy objective. Obstacles to resilience are seen as problems to be tackled, overcome or worked around. Resilience is life-affirming; lack of resilience results in disaster or death, or in the violation of human rights and freedoms. Not being resilient is a misfortune that can be righted through the application of analysis and resources of many kinds. However, these terms – "resilience" and "resilient" – are often not defined, their attributes are often left without explanation, and their relationship to adverse events and the effect of these events on people is often ambiguous. This adds to their quality as "hooray" terms or slogans attached to the myriad contexts in which they are either advocated or observed. On the other hand, ways of promoting or protecting resilience are examined in detail, with recommendations, in a great number of UN reports, thus taking the term out of the idiom of simple approval and exhortation.

An example of a virtually undefined use of "resilience" or "resilient" can be found in a UN report on global sustainability and sustainable development that includes the word "resilient" twice in its title.[116] The closest this report comes to a definition is in seeing resilience as an aspect of adaptation, and thus as "the ability to cope with climate change and natural disasters, in particular those associated with droughts, sea-level rise, increased temperatures and extreme weather events".[117] Elsewhere, resilience is associated with social protection, disaster risk reduction, the ability to deal with stress and shocks, precautionary strategies to prevent adverse impacts, and "resilience planning".[118] In the same general area of global concern, the UN's Food and Agriculture Organization (FAO) has highlighted the need for strategies and policies to increase resilience to drought, with an emphasis on prevention and proactive drought management in the face of climate change, but it invokes no general definition.[119]

---

[116] United Nations Secretary-General's High-level Panel on Global Sustainability, *Resilient People, Resilient Planet: A future worth choosing*, United Nations, New York, 2012.
[117] Ibid., para. 134.
[118] Ibid., paras. 136-138.
[119] Food and Agriculture Organization, "UN lays foundations for more drought resilient societies: Meeting urges disaster risk reduction instead of crisis management", 15 March 2013. http://www.fao.org/news/story/tr/item/172030/icode/en/

On the other hand, reporting on disaster risk and resilience, a document associated with the UN International Strategy for Disaster Reduction (UNISDR) quotes the UNISDR's authoritative definition of resilience, laid down in 2009: "[T]he ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions."[120] The disasters in focus here are "predictable" weather and weather-related events (e.g., floods), as well as earthquakes and tsunamis. Emphasis is placed on data collection and analysis of evidence, as well as international co-operation, as part of a strategy of prevention, emergency preparedness, risk reduction and resilience building. Again quoting the UNISDR definition, a disaster is "[a] serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources".[121]

In the health field, there is further evidence of the pertinence of a "resilience" perspective and language in the UN's approach to pandemics. For example, UN Secretary-General Ban Ki-moon's address to the 62nd World Health Assembly observed that "[t]he spread of the H1N1 virus illustrates some of the fundamental truths of public health: It helps us better understand the challenge we face today: how do we build resilience in an age of unpredictability and interconnection?" The answer, he said, lies in the development of public health systems, advance planning, information and intelligence, and institutional co-ordination.[122]

In another important health issue, World Health Organization (WHO) documentation includes a popular, illustrated manual on dealing with a mental health crisis caused by accidents, natural and man-made disasters.[123] Using simplified language and cartoons, the Indian Red Cross Society manual depicts a cycle that goes through several elements: disaster, shock, protest, anger, depression, re-organisation, and new path. The "road to resilience" – which can be seen as the "bouncing back" of resilience – involves the development of "positive coping skill" through three ways:

---

[120] UN System Task Team on the Post-2015 UN Development Agenda, *Disaster risk and resilience – Thematic Think Piece*, May 2012, p. 3, note 1, http://www.un.org/millenniumgoals/pdf/Think%20Pieces/3_disaster_risk_resilience.pdf. The definition is from United Nations Office for Disaster Risk Reduction, *UNISDR Terminology and Disaster Risk Reduction*, Geneva, UNISDR, 2009, p. 24, http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf. The UNISDR's comment on this definition is: "Resilience means the ability to 'resile from' or 'spring back from' a shock. The resilience of a community in respect to potential hazard events is determined by the degree to which the community has the necessary resources and is capable of organizing itself both prior to and during times of need."

[121] UN System Task Team on the Post-2015 UN Development Agenda, *Disaster risk and resilience – Thematic Think Piece*, May 2012, p. 9, note 11.
http://www.un.org/millenniumgoals/pdf/Think%20Pieces/3_disaster_risk_resilience.pdf. See United Nations Office for Disaster Risk Reduction, *UNISDR Terminology and Disaster Risk Reduction*, Geneva, UNISDR, 2009, p. 9, http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf

[122] Ban Ki-moon, "Resilience and solidarity: our best response to crisis", Address to the 62nd World Health Assembly, 19 May 2009.
http://www.who.int/mediacentre/events/2009/wha62/secretary_general_speech_20090519/en/

[123] Indian Red Cross Society, *Crisis to Recovery: The Road to Resilience*, Disaster Mental Health and Psychosocial Care Manuals, Number 6.
http://www.who.int/mental_health/emergencies/8.2_key_resource_1_american_redcross2.pdf

> The first way is to rebuild relationships. By developing relationships the person reestablishes trust and a sense of belonging. Secondly maintain day to day activities. Then each person identifies a safe place to rebuild confidence and competence in daily life. With children this occurs in school, with adults this can be done through participation in the reconstruction. Thirdly encourage a sense of spirituality. This is done by attempting to attribute meaning to the distressful event, rediscover hope in the future, and to find spiritual support. Relationships, activities and spirituality are linked to [a] person's inner resources. The capacity to use these inner resources is resilience.[124]

"Resilience" is defined as "the capacity to manage oneself when faced with difficult circumstances, to transform oneself in a positive way, and to recover from the distressful event and survive."[125] The manual gives step-by-step advice to persons and communities on how to recover from such crises and rebuild their lives. Successful recovery involves problem diagnosis, roles, plans, activities, resources, responsibilities, and – above all – being "positive about the future". There is less emphasis on crisis-prevention or preparedness in this approach than in other UN health materials. In one of these, natural and man-made disasters are seen as producing crises that strip people of their resilience and make them poor. This can be reversed by "[u]sing preparedness thinking to be aware of risks, to reduce them, and to plan ahead to combat them."[126] However, if preparedness is an anticipatory resilience strategy, the use of the same term to describe the stripping effect of crises on people is somewhat fuzzy.

It is not easy to find evidence of the use of 'resilience' in UN materials in relation to issues that are closer to the substantive concerns of IRISS. However, the question of the resilience of human rights in face of counter-terrorism is addressed in a non-UN research paper that aims to define a role for UN agencies in the human rights treaty-monitoring field.[127] The resilience in question is that of human rights norms that vulnerable to attack or relegation in the name of fighting terrorism, but the role of surveillance in counter-terrorism is not discussed. Nor is the right to privacy specifically mentioned as one that requires protection from counter-terrorist activities, although the author of the research paper considers the UN's position in relation to freedom from discrimination, and the discriminatory effects of profiling and stereotyping of supposed terrorists. These are noted as problems for the protection of human rights. To the extent that surveillance is involved in the collection and analysis of information that can be turned to discriminatory purposes, it could be argued that surveillance should come within the scope of UN treaty-monitoring in the midst of counter-terrorism, but the author of the paper does not take up this point, and indeed it would be hard to find direct, substantial discussion of surveillance and resilience to counter-terrorism surveillance through this route.

---

[124] Ibid., p. 6.
[125] Ibid.
[126] E.g., Inter-Agency Standing Committee, Sub-Working Group on Preparedness, *Preparedness: Saves Time, Money and Lives*, May 2011.
http://www.who.int/hac/network/interagency/news/iasc_preparedness_saves_time_money_lives.pdf
[127] Yusuf, Salma, "The Resilience of the Human Rights Norm in an Era of Counter-Terrorism", Research Unit on International Security and Cooperation (UNISCI), UNISCI Discussion papers No. 28, Madrid, January 2012.
http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=143780. UNISCI is not connected to the UN.

However, the UN Security Council's Counter-Terrorism Committee (CTED) held a Special Event on countering terrorism through the use of new information and communication technologies (ICTs), including the prevention and suppression of terrorism, which emphasized due regard for human rights and privacy protection in the use of mobile telephony for surveillance and monitoring.[128] The proactive, preventive and anticipatory use of ICTs against terrorists' exploitation of ICTs to further their aims was seen as essential, provided that States' use of such technologies "does not contravene human rights, the individual right to privacy, or the rule of law", as the Special Event's Chair urged in his opening statement.[129] This was echoed in the statement by the CTED Deputy Executive Director outlining the topics for the Special Event: tracking communications and the transfer of funds, including location, through mobile telephony; border-control systems for verifying passengers' identities with iris and digit scans; and monitoring and identifying terrorists on the Internet and in online social networks.[130]

Although "resilience" was not a term specifically used in the Special Event's discourse, its meaning was present in the focus upon counter-terrorism ICT measures and in the concern for the rule of law and human rights in the midst of this surveillance campaign. A similar concern can be found elsewhere in the UN's work – for example, in the mainstreaming of human rights in the field of drug control, crime prevention and criminal justice: "responses to crime, drugs and terrorism must be sure to protect the rights of vulnerable individuals who risk becoming the subject of criminal law and penalties".[131] Such sentiments can be interpreted as foregrounding human rights and the rule of law as tools for resilience asserting pressure against the achievement of the aims of law-enforcement and counter-terrorism missions where the latter pose a threat to other human rights and values. The position of surveillance in this threat is not elaborated.

Analysis from the IRISS perspective

From the IRISS point of view, some lessons can be learnt from this non-comprehensive canvass of the UN's perspective on resilience:

- The use of the term is not always evident although its connotation may be clear in terms of strategy and practical measures.
- Where the term is absent in a particular field, it is possible to construct a plausible scenario of resilience that identifies the threat, what is threatened, and how the threat can be countered through preventive or remedial measures.
- Preventative and preparedness measures – not the same thing – loom large in UN discourse across a range of fields and threats where threats or adverse events vary in terms of their inevitability, and therefore in the nature and dynamics of resilience.

[128] The Special Event was held on 24 May 2013. http://www.un.org/en/sc/ctc/news/2013-05-30_Special_Event_New_Tech.html
[129] http://www.un.org/en/sc/ctc/docs/2013/2013-05-24_opening_stmt_chair.pdf
[130] http://www.un.org/en/sc/ctc/docs/2013/2013-05-24_opening_stmt_CTED.pdf
[131] UN Commission on Narcotic Drugs/Commission on Crime Prevention and Criminal Justice, "Drug control, crime prevention and criminal justice: A Human Rights perspective" (Note by the Executive Director), E/CN.7/2010/CRP.6–E/CN.15/2010/CRP.1, 3 March 2010. http://www.unodc.org/documents/commissions/CND-Uploads/CND-53-RelatedFiles/ECN72010_CRP6eV1051605.pdf, para.15.

- In some fields in which surveillance features in the UN's discourse and work, it is easier to understand resilience even where the concept is not used or where such scenario-construction is difficult; however, "resilience to surveillance" is more elusive.
- All the above require interpretive skills in the conduct of IRISS research, more than relying on practitioners using terminology and concepts that are clear-cut and plainly applicable in the minds of researchers.

2.1.6 Resilience in public transport systems

Dr Reinhard Kreissl, Institute for the Sociology of Law and Criminology (IRKS)

Public transport systems in metropolitan areas display a number of features that highlight some general points relevant for the discussion of resilience.

First of all, public transport systems are complex, open and hence vulnerable. Second, they operate on time-critical processes, i.e., any disturbance of smooth processing immediately triggers secondary effects cascading over the whole system. These two properties are highly relevant when investigating the problem of resilience. A strategy such as target hardening is not feasible for a system such as public transport in metropolitan areas, since these systems are "soft" targets. Major attacks cannot be prevented by controlling access to train stations or vehicles or mounting more technical surveillance systems within the system's premises. It is also difficult to identify and locate major attacks in the system, since the centralised information-processing unit of large transport systems handles a huge amount of highly heterogeneous information in real time. Minor disturbances are frequent and do not trigger a major alarm. Major attacks somewhere in the system (e.g., a bomb attack or the release of lethal gas in a train) surface in the control centres as "black out" of CCTV monitors or a report on customers complaining about dizziness – i.e., as a series of isolated "minor events". Typically, it takes a few minutes for the control centre operators to combine the information from different sources (Intercom, CCTV, sensors, etc.) to identify a minor disturbance or technical failure as an event pointing to a serious incident.

With regard to resilience, this peculiar situation with a "blind centre of decision" working on an input from remote distributed sensors and handling different sources of information suggests to focus on the structure of communication and perception in this very centre. How do the operators tied into a regime of cognitive division of labour forming what could be called a system of distributed collective cognition distinguish between a string of single trivial incidents and a major physical attack on their system? When do they decide to take a black-out of two CCTV cameras not as a technical failure but as the effect of a bomb blast in the station where these cameras are mounted? Technical failures of this type are common in the daily routine operation, whereas a major attack is more similar to a black swan event, unexpected and with a very low probability. Typically, a control centre operator, based on his or her experience, will interpret a series of mundane failures as trivial problems. Working in an environment of technical (surveillance) systems, operators come to expect minor disturbances.

What this demonstrates clearly is a problem that could be termed the problem of the human bottleneck. Modern metropolitan public transport systems are densely under surveillance, from pervasive CCTV to different types of sensors, to a variety of other channels from Intercom to mobile phones. Users and staff can contact the control centres through low-threshold communication channels to report what they deem important. This complex information combines into a communication overload at the receiving end, where the operators of the control centre are performing their task of keeping a smooth flow of traffic going. Typically, each operator has assigned a specific task or a geographical segment of the overall system and has to co-ordinate with his or her co-workers. This co-ordination *within* the control centres has not received adequate attention when investigating resilience of public transport systems.

A resilient public transport system hence would be one where information is processed in a way that allows for the identification of critical events, i.e., reducing the "noise" coming from different sources.

2.1.7 Civil protection in a European context

Charles Leleux, University of Stirling

The term "civil protection" has different meanings and interpretations, sometimes varying from country to country. In the context of Europe, civil protection and its developing and multi-faceted relationship with resilience is a relatively recent phenomenon, arguably originating from the end of the cold war, commonly described as the period from the end of World War II to the early to mid-1990s,[132] when the focus changed to civil protection from civil defence, with contingency plans being put in place by many countries for the civilian populations to organise, prepare to mobilise and defend themselves in the event of a major incident such as a nuclear attack or potential invasion by another country. Over the past two to three decades, and at the level of the European Union, the use of the term "civil protection"[133] has become synonymous with the contingency and emergency planning arrangements that countries either individually and now increasingly collectively (such as the six regional European civil protection initiatives)[134] have put in place to increase resilience and the ability to respond effectively both to the threat or occurrence of natural disasters, such as earthquakes and damage to the built environment,[135] volcanic eruptions,[136] forest fires,[137] floods,[138] landslides and man-made disasters

[132] LaFeber, Walter, *America, Russia, and the Cold War, 1945-1996*, McGraw-Hill, New York, 1997.
[133] European Commission, Communication from the Commission to the European Parliament, and the Council on a proposal for a decision on a Union Civil Protection Mechanism, COM (2011) 934 final, Brussels, 20.12.2011.
http://ec.europa.eu/echo/files/about/COM_2011_proposal-decision-CPMechanism_en.pdf
[134] European Commission, Humanitarian Aid & Civil Protection, European Civil Protection, International Co-operation. http://ec.europa.eu/echo/civil_protection/civil/prote/cp11_en.htm.
[135] Alexander, David E., "The L'Aquila earthquake of 6 April 2009 and Italian Government policy on disaster response", *Journal of Natural Resources Policy Research*, Vol. 2, No. 4, 2010, pp. 325-342. See also Amaratunga, Dilanthi, and Richard Haigh (eds.), *Rebuilding for Resilience: Post-Disaster, Reconstruction of the Built Environment*, Wiley-Blackwell, 2011.
[136] Sangster, H., D.K. Chester and A. M. Duncan, "Human responses to historical eruptions of Etna (Sicily) from 1600 to present and their implications for present-day disaster planning", *Conference Proceedings*, EGU General Assembly 2012, held 22-27 April 2012 in Vienna, p. 8477.
[137] European Commission, *JRC Scientific and Technical Reports*, Forest fires in Europe 2008, No.9, 2009.

such as marine pollution incidents or threats or actual acts of terrorism such as those experienced in London (2005) or Madrid (2004).[139] Gestri identified the mid-1980s as the period which saw the beginning of an organised and collective approach to civil protection in Europe: "On the European plane, the first step towards the introduction of forms of cooperation on civil protection was a meeting in Rome, at ministerial level, in May, 1985."[140] Gestri also recognised a weakness in the ability to organise any collective approach to this developing subject area, due to the lack of a legislative structure: ''However, before the entry into force of the Treaty of Lisbon and the further development of a European response, capacity was limited by the absence of an adequate legal basis.''[141] The Treaty of Lisbon,[142] which was signed in 2007, and came into force in 2009, introduced changes to civil protection, through increasing co-operation amongst Member States for preventing and protecting against natural or man-made disasters. The European Union determined that increasing preparedness and resilience to natural or man-made disasters or to terrorism events would require greater humanitarian focus and co-ordination of resources at a community-based level. In response to this, the European Union adopted two pieces of legislation which cover European civil protection: first, Council Decision 2007/779/EC established a Community Civil Protection Mechanism[143] and, second, Council Decision 2007/162/EC established a Civil Protection Financial Instrument.[144] The Mechanism covers the response and some preparedness activities, while the Instrument enables actions in the three key areas of prevention, preparedness and response.

The Barnier Report proposed the creation of a European Civil Protection Force,[145] the case for which, it has been argued, arose out of the European Security and Defence Policy, adopted in 1999,[146] and possibly from the inability of Europe to co-ordinate an effective response to the Kosovo crisis of 1999.[147] The European Union has, as a

---

http://forest.jrc.ec.europa.eu/media/cms_page_media/9/forest-fires-in-europe-2008.pdf.

[138] Del Carmen, Llasat, and F. Siccardi, "A reflection about the social and technological aspects in flood risk management–the case of the Italian Civil Protection", *Natural Hazards Earth Systems Science*, Vol. 10, No. 1, 2010, pp. 109-119.

[139] Canel, José Maria, and Karen Sanders, "Crisis communication and terrorist attacks: framing a response to the 2004 Madrid bombings and 2005 London bombings", in W. Timothy Coombs and Sherry J. Holladay (eds.), *The handbook of crisis communication*, Wiley-Blackwell, Chichester (UK), 2010, pp. 449-466.

[140] Gestri, Marco, *EU Disaster Response Law: Principles and Instruments*, Springer, 2012, pp. 105-128.

[141] Ibid., p. 105.

[142] European Commission, "The Treaty of Lisbon", EUROPA website, 1 December.2009.http://europa.eu/lisbon_treaty/index_en.htm.

[143] European Commission, Euratom: Council Decision of 8 November 2007 establishing a Community Civil Protection Mechanism.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0779(01):EN:NOT.

[144] European Commission, 2007/162/EC, Euratom: Council Decision of 5 March 2007 establishing a Civil Protection Financial Instrument.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0162:EN:NOT.

[145] Barnier, Michel, *For a European civil protection force: europe aid*, European Commission, Humanitarian Aid and Civil Protection, European Civil Protection, May 2006.
http://ec.europa.eu/archives/commission_2004-2009/president/pdf/rapport_barnier_en.pdf

[146] Deighton, Anne, "The European security and defence policy", *JCMS: Journal of Common Market Studies*, Vol. 40, No. 4, 2002, pp. 719-741.

[147] Bailes, Alyson J.K., "The EU and a 'better world': what role for the European Security and Defence Policy?", *International Affairs*, Vol. 84, No. 1, 2008, pp. 115-130, See also Berinsky, Adam J., Donald R. Kinder, "Making sense of issues through media frames: Understanding the Kosovo crisis", *Journal of Politics*, Vol. 68, No. 3, 2006, pp. 640-656.

consequence of major events, such as the fires of southern Europe in 2007,[148] produced various Communications aimed at increasing the level of community response, such as COM (2009) 82 final, which reinforces the input and therefore resilience required to be shown by communities ''This Communication follows up on the commitment made by the Commission to develop proposals on disaster prevention and responds to the calls of the European Parliament and the Council for increased action at Community level to prevent disasters and mitigate their impacts.''[149] The role of the European Union in civil protection and resilience has purposely been extended, to now include humanitarian aspects,[150] and is intended to reach beyond the boundaries of the European Union itself to other parts of the world, such as with the assistance provided following the earthquake and tsunami in Japan (2011), the Christchurch earthquake in New Zealand (2011), and the evacuation of EU citizens from Libya (2011). The European Union describes its role in relation to civil protection in the following terms:

> The fundamental approach to an effective civil protection operation relies on three key modes of action: Prevention, Preparedness & Response. The European Commission is responsible for supporting and supplementing efforts at national, regional and local level with regard to disaster prevention, the preparedness of those responsible for civil protection and the intervention in the event of disaster.[151]

An example of the European Union's response (in civil protection terms) to an adverse event, the major flooding which hit Slovenia in 2012, can be found in the statement made on 30 April 2013 by the European Commissioner for Regional Policy, Johannes Hahn, who "announced an aid package from the EU Solidarity Fund (EUSF) of over €14.6 million in response to serious flooding in Slovenia in October and November 2012".[152]

The European Union's response to civil protection and resilience

The European Union's response to civil protection and resilience is embedded in solidarity: "Our aim is to boost solidarity among Member States and our neighbouring countries so as to achieve the optimal level of preparedness for emergencies and to

---

[148] European Commission, *JRC Scientific and Technical Reports*, Forest fires in Europe 2008, No.9, 2009, http://forest.jrc.ec.europa.eu/media/cms_page_media/9/forest-fires-in-europe-2008.pdf.

[149] European Commission, A Community approach on the prevention of natural and man-made disasters, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, OM (2009) 82 final, Brussels, 23 Feb 2009.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2009:0202:FIN:EN:PDF.

[150] European Commission, Communication from the Commission to the European Parliament, and the Council, Towards a stronger European disaster response: the role of civil protection and humanitarian assistance, COM (2010) 600 final, Brussels, 26 Oct 2010.
http://ec.europa.eu/echo/civil_protection/civil/prote/pdfdocs/COM_2010_600_European_disaster_response_en.pdf.

[151] European Commission, Humanitarian Aid & Civil Protection, European Civil Protection, Community co-operation in the field of civil protection, 1 Dec 2011.
http://ec.europa.eu/echo/civil_protection/civil/prote/cp01_en.htm.

[152] European Commission, Johannes Hahn, "European Commissioner for Regional Policy", News release, 30 Apr 2013. http://ec.europa.eu/commission_2010-2014/hahn/headlines/news/detail/index_en.cfm?LAN=EN&id=696&lang=en.

ensure a rapid and effective response when disaster strikes."[153] The "solidarity" commitment is also contained in the Treaty of Lisbon.[154] However, some commentators have raised concerns over the ability of Member States to co-operate with each other in the best interests of a collective response, due to issues connected to sovereignty, and in relation to potential overlaps between solidarity clauses and collective defence clauses.[155]

The European Commission defines resilience as "the ability of an individual, a household, a community, a country or a region to withstand, adapt, and quickly recover from stresses and shocks such as drought, violence, conflict or natural disaster."[156] The European Commission has recognised the growing importance of the need to focus on resilience as a key component for collectively organised humanitarian aid in times of natural disasters or major events caused by other factors such as terrorism: "Strengthening resilience lies at the crossroads between humanitarian and development assistance. With this in mind the European Commission has proposed a new policy Communication to the European Parliament and the Council on how EU development and humanitarian aid should be adapted to increase the resilience and reduce the vulnerability of people affected by disasters."[157] The European Commission has identified increasing resilience as a priority in three key areas: food security, climate change adaptation and disaster risk reduction. The new resilience Communication outlines 10 steps "that will increase resilience and reduce the vulnerability of the world's most vulnerable people. These steps include support for the design of national resilience strategies, disaster management plans and efficient early-warning systems in disaster-prone countries, as well as putting forward innovative approaches to risk management through collaboration with the insurance industry." [158]

Community Mechanism for civil protection

Demonstrating the importance of the engagement of communities in the role of civil protection and resilience, the European Union established the Community Mechanism for Community Protection in 2001. Now with 31 Member States, each of which has their own civil protection structures, the Mechanism has a declared purpose:

> to facilitate reinforced cooperation between the Community and the Member States in civil protection assistance intervention in the event of major emergencies, or the

[153] European Commission, Humanitarian Aid & Civil Protection, European Civil Protection, Consultation on the Future Instrument Addressing Prevention of, Preparedness for and Response to Disasters. http://ec.europa.eu/echo/civil_protection/civil/consult_new_instrument.htm.
[154] European Commission, official website of the European Union, EUROPA, The Treaty of Lisbon, 1 Dec 2009. http://europa.eu/lisbon_treaty/index_en.htm.
[155] See, respectively, Ekengren, Magnus, Nina Matzén, Mark Rhinard and Monica Svantesson, "Solidarity or sovereignty? EU cooperation in civil protection", *European Integration*, Vol. 28, No. 5, 2006, pp. 457-476; Konstadinides, Theodore, "Civil Protection in Europe and the Lisbon 'solidarity clause': A genuine legal concept or a paper exercise", *Juridiska fakulteten*, Uppsala Universitet, 2011.
[156] European Commission, Humanitarian Aid & Civil Protection, Policies and Operations, Resilience. http://ec.europa.eu/echo/policies/resilience/resilience_en.htm.
[157] European Commission, The EU Approach to Resilience: Learning from Food Security Crises, Communication from the Commission to the European Parliament, and the Council, COM (2012) 586 final, 3 Oct 2012.
http://ec.europa.eu/europeaid/what/food-security/documents/20121003-comm_en.pdf.
[158] Ibid.

> imminent threat thereof. The protection to be ensured by the Mechanism shall cover primarily people but also the environment and property, including cultural heritage, in the event of natural and man-made disasters, acts of terrorism and, technological, radiological or environmental accidents, including accidental marine pollution, occurring inside or outside the Community, taking also into account the special needs of the isolated, outermost and other regions or islands of the Community.[159]

In terms of its response to major events since 2001, the Mechanism has been brought into operation more than 150 times, for a variety of major events, both within and beyond the European Union including the tsunami in South Asia (2004/2005); Hurricanes Katrina and Rita in the USA (2005); earthquakes in China (2008), Haiti (2010), Japan (2011); floods in the Balkans (2010); forest fires in Greece (2007, 2012); civil unrest in Libya (2011); and an explosion at a naval base in Cyprus (2011).[160] In responding to major events, the Community Mechanism for Civil Protection uses administrative and operational instruments, which have the twin aims of achieving suitable readiness and appropriate action at the community level. These instruments, or tools, include, first, the Monitoring Information Centre (MIC), which is accessible 24 hours a day, and "gives countries access to a platform, to a one-stop-shop of civil protection means available amongst all the participating states. Any country inside or outside the Union affected by a major disaster can make an appeal for assistance through the MIC. The MIC acts as a communication hub at headquarters level between participating states, the affected country and despatched field experts."[161] Second, the Common Emergency and Information System is a Web-based alert and notification application for facilitating emergency communication amongst the participating states. Third, a training programme has been devised for "improving the co-ordination of civil protection assistance interventions by ensuring compatibility and complementarity between the intervention teams from the participating states."[162] Finally, civil protection "modules" draw on "national resources from one or more Member States on a voluntary basis. These "modules" are contributions to the civil protection rapid response capability called for by the European Council in its Conclusions in December 2005[163] and by the European Parliament in its Resolution in January 2005 on the tsunami disaster.[164]

It can be seen that the role of the European Union in developing civil protection and increasing resilience, since the mid-1980s, has been a developing one, and is one that is increasingly based on a collective, community and humanitarian response to achieve maximum effect, and is not confined to the borders of the Member States.[165]

---

[159] European Commission, 2007/779/EC, Euratom: Council Decision of 8 November 2007 establishing a Community Civil Protection Mechanism. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0779(01):EN:NOT

[160] European Commission, Humanitarian Aid & Civil Protection, Disaster Response, The community mechanism for civil protection. http://ec.europa.eu/echo/policies/disaster_response/mechanism_en.htm

[161] Ibid.

[162] Ibid.

[163] European Commission, Official Journal of the European Union, Council conclusions on improving European civil protection capabilities, Notice No. 2005/C, 304/01, 1.12.05, http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2005:304:SOM:en:HTML.

[164] European Commission, Council of Europe, Parliamentary Assembly, Europe and the Tsunami Disaster, Resolution 1422, 26.1.2005, http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta05/ERES1422.htm.

[165] European Commission, Humanitarian Aid & Civil Protection, European Civil Protection, International Co-operation. http://ec.europa.eu/echo/civil_protection/civil/prote/cp11_en.htm See also

The principle of subsidiarity also guides the European Union's responses, in that actions should occur at the most local level possible.

Other institutions involved in civil protection at a European level

Responsibility for intervening in European regional civil protection assistance and increasing resilience to the occurrence of major events is not the sole preserve of the European Commission or the European Parliament. The South Eastern Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP)[166] is a collaborative initiative developed by the World Bank and the United Nations International Strategy for Disaster Reduction Secretariat (UNISDR) in co-operation with international and regional partners, which include the European Commission (EC); Council of Europe (European and Mediterranean Major Hazards Agreement); Regional Coordination Council for South Eastern Europe (RCC SEE); Disaster Preparedness and Prevention Initiative for South Eastern Europe (DPPI SEE); and UN partners including the World Meteorological Organization (WMO), the United Nations Office for the Co-ordination of Humanitarian Affairs (OCHA) and the United Nations Development Programme (UNDP). SEEDRMAP aims at lessening the susceptibility of South Eastern Europe (SEE) to the risk of disasters, and considers the insurance, risk and financial recovery aspects of preparing for and responding to disasters:

> It addresses the loss of life, property and economic productivity caused by weather extremes and other natural hazards in the context of the implementation of the Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters. To that end, SEEDRMAP has three focus areas: (i) hydrometeorological forecasting, data sharing and early warning; (ii) coordination of disaster mitigation, preparedness and response; and (iii) financing of disaster losses, reconstruction and recovery, and of disaster risk.[167]

The United Kingdom, civil protection and resilience

The United Kingdom has a reasonably robust system of civil protection and resilience, developed over the years since the end of the Second World War, ranging from volunteer organisations at the local level up to national response bodies such as the emergency services (police, fire and rescue and ambulance services), and ultimately respective national governments. The Civil Contingencies Act 2004 (CCA)[168] defines an emergency as an event or situation which threatens serious damage to human welfare or the environment in the UK or a war or terrorism, which threatens the security of the UK.[169] Civil protection in the United Kingdom is provided for by the CCA, which has two main parts: Part 1 of the Act, and the

---

European Commission, Communication from the Commission to the European Parliament, and the Council Towards a Stronger European Disaster Response: The Role of Civil Protection and Humanitarian Assistance, COM (2010) 600 final, Brussels, 26 October 2010.

[166] The South Eastern Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP). http://www.unisdr.org/files/18135_seedrmapbrochure.pdf.

[167] Ibid.

[168] UK Government, Civil Contingencies Act, 2004, 18 Nov 2004. http://www.legislation.gov.uk/ukpga/2004/36/contents.

[169] Ibid.

Contingency Planning Regulations, 2005[170] and Contingency Planning (Scotland) Regulations, 2005[171] establish the roles and responsibilities for organisations involved in emergency preparation and response, and Part 2 provides the legislative basis upon which to make emergency regulations, the scope of these regulations, their duration and arrangements for Parliamentary scrutiny. The CCA establishes a statutory framework for civil protection and resilience-building at the local level, setting out roles and responsibilities for local responders. The CCA Part 2 also provides the scope to impose a duty on the designated emergency responders to assess, plan and advise in relation to preventing the emergency, reducing, controlling or mitigating its effects, undertaking exercises and training staff.[172] The CCA designates responders in terms of Category One or Two. Category One responders include the national emergency response services such as police, fire and rescue services, National Health Service and ambulance services, while Category Two responders include utility companies such as gas, electricity, water, sewerage and public electronic communications as well as transport, railways, airports and the Health and Safety Executive (HSE).

The UK government provides guidance on emergency planning, resilience and preparedness; exercises and training; national recovery guidance on humanitarian issues, economic issues, infrastructural issues, plus telecoms resilience.[173] The Government's resilience to major events has been demonstrated at a national level through the establishment of the highly publicised civil emergencies committee, commonly known as the COBRA Committee (Cabinet Office Briefing Room A),[174] which is normally chaired by the Prime Minister, and meets when required to deal with civil emergencies and terrorism alerts. The Cabinet Office provides advice to individuals and networks in the form of a guide on Integrated Emergency Management (IEM)[175] which covers "anticipation, assessment, prevention, preparation, response and recovery. Resilience is about all these aspects of emergency management, and this guide deals with the resilience of existing entities in the UK such as buildings, systems and networks."[176] The guide also covers community resilience. In Scotland, the Scottish Government's Resilience Division supports the frontline agencies that deliver emergency planning and response across Scotland.[177]

---

[170] UK Government, Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005, No. 2042, Part 7, Reg. 40. http://www.legislation.gov.uk/uksi/2005/2042/regulation/40/made.
[171] UK Government, Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005, 14 Nov 2005. http://www.legislation.gov.uk/ssi/2005/494/contents/made.
[172] Ibid.
[173] UK Government, Cabinet Office, *Inside Government, Public safety and emergencies, What we're doing*, https://www.gov.uk/government/topics/public-safety-and-emergencies. See also UK Government, National recovery guidance, generic issues: social media, London, 4 Oct 2012, https://www.gov.uk/government/publications/national-recovery-guidance-generic-issues-social-media.
[174] UK Government, Cabinet Office, "Inside Government, COBRA meeting on fuel". https://www.gov.uk/government/news/cobra-meeting-on-fuel-contingencies.
[175] UK Government, Cabinet Office, "Resilience in society: infrastructure, communities and businesses". https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses#corporate-resilience-sme-resilience-strategy.
[176] Ibid.
[177] Scottish Government, Safer Scotland, Ready Scotland, "Preparing for and dealing with emergencies, Resilience Division". http://www.readyscotland.org/ready-government/resilience-division/.

The Resilience Advisory Board,[178] which normally meets three times per annum, provides advice to Scottish Ministers and the wider civil contingencies community on strategic policy development. Membership of the Resilience Advisory Board includes representation from the public, private and voluntary sectors, and organisations which are representative of Category One and Two responders in terms of the CCA, such as the Chief Fire Officers' Association (Scotland); the Association of Chief Police Officers' Scotland (ACPOS); the Scottish Ambulance Service; NHS Scotland; the Society of Local Authority Chief Executives; the Convention of Scottish Local Authorities; the Scottish Environmental Protection Agency; Scottish Power; Network Rail and the Met Office.[179] The Scottish Resilience Development Service (ScoRDS) is part of the Resilience Division and provides "training, exercising and other knowledge development opportunities to the emergency services and other responder agencies, to ensure that Scotland is prepared to respond to any major emergency." [180]

Community engagement in the UK

The Civil Contingencies Act, 2004,[181] the Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005[182] and the Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005[183] establish, inter alia, how Category One and Two responders should engage with voluntary organisations in assisting them in responding to civil emergencies. The legislation and Government guidance imposes a duty on the responders to make best use of local resources, and sets out what their responsibilities are.[184] In responding to civil emergencies, the voluntary sector often plays a crucial role, as the resources of the Category One and Two responders will undoubtedly be stretched in attending to the emergency, whilst still needing to maintain their mainstream operational roles. The UK Government, Cabinet Office, has established the Voluntary Sector Civil Protection Forum, which is a grouping of voluntary organisations that have a civil protection role, and provides advice.[185] For example, the Norfolk Civil Protection Volunteers[186] provide support to Broadland and North Norfolk District Councils and the Emergency Services when they have an emergency. Combining the interests of the business community and voluntary and

[178] Scottish Government, Safer Scotland, Ready Scotland, "Preparing for and dealing with emergencies, Resilience Advisory Board".
http://www.readyscotland.org/ready-government/resilience-advisory-board/
[179] Ibid.
[180] Scottish Government, Safer Scotland, Ready Scotland, "Preparing for and dealing with emergencies, ScoRDS".
http://www.readyscotland.org/ready-government/scords/.
[181] UK Government, Civil Contingencies Act, 2004, 18 Nov 2004.
http://www.legislation.gov.uk/ukpga/2004/36/contents
[182] UK Government, Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005, No. 2042, Part 7, Reg. 40. http://www.legislation.gov.uk/uksi/2005/2042/regulation/40/made
[183] UK Government, Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005, 14 Nov 2005. http://www.legislation.gov.uk/ssi/2005/494/contents/made. In exceptional circumstances, emergency powers may also be available. For further details, see UK Government, Cabinet Office.
http://www.cabinetoffice.gov.uk/content/civil-contingencies-act
[184] UK Government, Cabinet Office, *Preparation and planning for emergencies: responsibilities of responder agencies and others*, February 2013. https://www.gov.uk/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others
[185] UK Government, Cabinet Office, *Guidance, Voluntary Sector Civil Protection Forum*, 2012.
https://www.gov.uk/government/publications/voluntary-sector-civil-protection-forum-2012
[186] Norfolk Civil Protection Volunteers. http://www.norfolkcivilprotection.org.uk/

public sector organisations, Community Resilience UK cic[187] is a not-for-profit company which helps people and their communities prepare for and recover from major emergencies. It works with the business community and voluntary and public sector organisations.

Preparedness and resilience

Many public agencies in the UK, such as local authorities and health services, often organise emergency planning exercises involving a multi-agency approach, followed by debriefing and "lessons learned" dissemination. The focus of these training events, and preparations in general, is not necessarily on the cause(s) of the adverse event, but rather on the adequacy of the response, the effectiveness of communications, the resilience capacity of the responders, the establishment of a suitable control centre, the success of inter-agency co-operation, the visibility and awareness of the command structure, and the suitability of the deployment of resources. Taking the emergency planning arrangements put in place by a local authority in central Scotland, e.g., South Lanarkshire Council, which has more than 14,000 employees and a population of around 300,000, they have a contingency planning officer[188] and an Emergencies Management Team comprising various contingency planning officers across all departments of the Council, each ready to be alerted at any time in the event of an emergency. To enable a swift response to any emergencies, South Lanarkshire Council has prepared an emergency planning handbook, containing names, home addresses, home telephone numbers and mobile telephone numbers of all senior management personnel, and facilities managers, which has been issued to all designated contacts and senior management teams. Many emergency planning officials in the UK are members of a professional body, such as the Institute of Civil Protection and Emergency Management (ICPEM).[189]

In conclusion, one can see that the basis of the UK's response to civil protection, and resilience capacity-building, stems from an acceptance that it would be probably be impossible for a single body acting unilaterally to deal competently with the complex demands of a civil emergency. The UK advocates a collective approach involving agencies working collaboratively and engaging with the community and voluntary sectors.

General comments from an IRISS project perspective

In the domain of civil protection, the term "resilience" has been used widely by the European Commission and European Parliament, and by the United Kingdom and Scottish governments. Particular attention has been given to the development of the response by communities and the voluntary sector to natural or man-made disasters, and this has been mirrored both at the European Union and United Kingdom government levels. Resilience capacity building has had an increasing focus at a European Union level since the late 1990s, extending in recent years to humanitarian

[187] Community Resilience UK cic. http://communityresilience.cc/. Cic stands for Community Interest Company.
[188] The author acknowledges, with thanks, information supplied by the Contingency Planning Officer of South Lanarkshire Council for this section.
[189] The Institute of Civil Protection and Emergency Management (ICPEM), http://www.icpem.net/. The ICPEM is affiliated with the International Civil Defence Organisation, www.icdo.org.

assistance. Examples of this increased focus can be found in: a) legislation in force (e.g. the establishment of a Community Civil Protection Mechanism);[190] b) implementing rules; c) Council conclusions; d) European Parliament Resolutions, and e) through various Communications from the European Commission to the European Parliament, the Council and Committees. The European Commission has also identified increasing resilience as a priority in three key areas: food security, climate change adaptation, and disaster risk reduction. Similarly, in the United Kingdom resilience capacity building has been the subject of legislation (through the Civil Contingencies Act, 2004 and the subsequent Regulations, 2005), where Category One responders (e.g., police, fire and rescue and ambulance services) are required in civil emergency situations to make best use of community and voluntary resources. The United Kingdom Government Cabinet Office has also issued advice and guidance relating to responder agencies, infrastructure, communities, businesses, and the voluntary sector. The Scottish Government has embedded the term resilience within its support structure for responding to civil emergencies, through its Resilience Division which supports the frontline agencies that deliver emergency planning and response across Scotland,[191] and the Resilience Advisory Board,[192] which normally meets three times per annum, providing advice to Scottish Ministers and the wider civil contingencies community on strategic policy development.

A fundamental question remains as to the extent to which the increased focus on resilience capacity-building depends upon surveillance systems and technologies. Undoubtedly, greater and more sophisticated use is made of systems for monitoring volcanic activity, and the potential for flooding, for example, the South Eastern Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP)[193] has as one of its stated priorities, hydrometeorological forecasting, data sharing and early warning. Similarly, the European Community Mechanism for Civil Protection uses administrative and operational instruments, one of which includes the Monitoring Information Centre (MIC),[194] which is accessible 24 hours a day, and acts as a communication hub at headquarters level between participating states, the affected country and despatched field experts. Clearly, the MIC depends to a large extent on the ability of its monitoring systems to provide easily accessible and accurate information. From the examples in the preceding paragraphs and elsewhere in this contribution, it can be asserted that the concept and term of resilience have clearly entered the policy-making discourse amongst governments, governmental bodies and practitioners, however, it is harder to assess the extent to which resilience has entered into the public discourse in society in general, and especially around the area of democratic processes. These aspects would require further examination.

---

[190] European Commission, 2007/779/EC, Euratom: Council Decision of 8 November 2007 establishing a Community Civil Protection Mechanism. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0779(01):EN:NOT

[191] Scottish Government, Safer Scotland, Ready Scotland, Preparing for and dealing with emergencies, Resilience Division. http://www.readyscotland.org/ready-government/resilience-division/

[192] Scottish Government, Safer Scotland, Ready Scotland, Preparing for and dealing with emergencies, Resilience Advisory Board. http://www.readyscotland.org/ready-government/resilience-advisory-board/

[193] The South Eastern Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP). http://www.unisdr.org/files/18135_seedrmapbrochure.pdf

[194] European Commission, Humanitarian Aid & Civil Protection, Disaster Response, The community mechanism for civil protection. http://ec.europa.eu/echo/policies/disaster_response/mechanism_en.htm

References

Alexander, David E., "The L'Aquila earthquake of 6 April 2009 and Italian Government policy on disaster response", *Journal of Natural Resources Policy Research*, Vol. 2, No.4, 2010, pp. 325-342.

Amaratunga, Dilanthi, and Richard Haigh (eds.) *Rebuilding for Resilience: Post-Disaster, Reconstruction of the Built Environment*, Wiley-Blackwell, Chichester, 2011.

Bailes, Alyson J. K., "The EU and a 'better world': what role for the European Security and Defence Policy?" *International Affairs,* Vol. 84, No. 1, 2008, pp. 115-130.

Barnier, Michel, *For a European civil protection force: Europe Aid, European Commission and the Council*, May 2006. http://ec.europa.eu/archives/commission_2004-2009/president/pdf/rapport_barnier_en.pdf

Berinsky, Adam J., and Donald R. Kinder, "Making sense of issues through media frames: Understanding the Kosovo crisis", *Journal of Politics,* Vol. 68, No. 3, 2006, pp. 640-656.

Canel, José Maria, and Karen Sanders, "Crisis communication and terrorist attacks: framing a response to the 2004 Madrid bombings and 2005 London bombings", in W. Timothy Coombs and Sherry J. Holladay (eds.) *The handbook of crisis communication*, 2010, pp. 449-466.

Community Resilience UK cic. http://communityresilience.cc/.

Council of Europe, Parliamentary Assembly, Europe and the Tsunami Disaster, Resolution 1422, 26.1.2005. http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta05/ERES1422.htm

Deighton, Anne, "The European security and defence policy", *JCMS: Journal of Common Market Studies,* Vol. 40, No. 4, 2002, pp. 719-741.

Del Carmen, Llasat, and F. Siccardi, "A reflection about the social and technological aspects in flood risk management – the case of the Italian Civil Protection", *Natural Hazards Earth Systems Science*, Vol. 10, 2010, pp.109-119.

Ekengren, Magnus, Nina Matzen, Mark Rhinard and Monica Svantesson, "Solidarity or sovereignty? EU cooperation in civil protection", *European Integration,* Vol. 28, No. 5, 2006, pp. 457-476.

European Commission, A Community approach on the prevention of natural and man-made disasters, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2009) 82 final, Brussels, 23 Feb 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2009:0202:FIN:EN:PDF

European Commission, Towards a stronger European disaster response: the role of civil protection and humanitarian assistance, Communication from the Commission to the European Parliament and the Council, COM (2010) 600 final, Brussels, 26.10.2010, http://ec.europa.eu/echo/civil_protection/civil/prote/pdfdocs/COM_2010_600_European_disaster_response_en.pdf

European Commission, Proposal for a decision of the European Parliament and of the Council on a Union Civil Protection Mechanism, COM (2011) 934 final, Brussels, 20.12.2011. http://ec.europa.eu/echo/files/about/COM_2011_proposal-decision-CPMechanism_en.pdf

European Commission, The EU Approach to Resilience: Learning from Food Security Crises, Communication from the Commission to the European Parliament and the Council, COM (2012) 586 final, 3.10.2012. http://ec.europa.eu/europeaid/what/food-security/documents/20121003-comm_en.pdf

European Commission, *JRC Scientific and Technical Reports*, Forest fires in Europe 2008, No.9, 2009. http://forest.jrc.ec.europa.eu/media/cms_page_media/9/forest-fires-in-europe-2008.pdf

European Commission, Humanitarian Aid & Civil Protection, European Civil Protection,

International Co-operation. 1 Dec 2011. http://ec.europa.eu/echo/civil_protection/civil/prote/cp11_en.htm

European Commission, Humanitarian Aid & Civil Protection, European Civil Protection, Community co-operation in the field of civil protection, last updated 1 Dec 2011. http://ec.europa.eu/echo/civil_protection/civil/prote/cp01_en.htm

European Commission, Humanitarian Aid & Civil Protection, Consultation on the Future Instrument Addressing Prevention of, Preparedness for and Response to Disasters, Last updated: 1 Dec 2011. http://ec.europa.eu/echo/civil_protection/civil/consult_new_instrument.htm

European Commission, Humanitarian Aid & Civil Protection, "Resilience", Last updated: 18 Dec 2012. http://ec.europa.eu/echo/policies/resilience/resilience_en.htm

European Commission, Humanitarian Aid & Civil Protection, "The community mechanism for civil protection", updated 17 Apr 2013. http://ec.europa.eu/echo/policies/disaster_response/mechanism_en.htm

European Commission Council conclusions on improving European civil protection capabilities, Official Journal of the European Union, C, 304/01, Vol. 48, 1 Dec 2005. http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2005:304:SOM:en:HTML

European Council, Council Decision of 5 March 2007 establishing a Civil Protection Financial Instrument, 2007/162/EC, *OJ L* 71, 10 March 2007, p. 9–17. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0162:EN:NOT

European Council, Council Decision of 8 November 2007 establishing a Community Civil Protection Mechanism, 2007/779/EC, Official Journal of the European Union, L314/9, 1 Dec 2007.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0779(01):EN:NOT

European Union, The Treaty of Lisbon, Official Journal of the European Union, 17 Dec 2009. http://europa.eu/lisbon_treaty/index_en.htm

Gestri, Marco, "EU Disaster Response Law: Principles and Instruments", in Andrea de Guttry, Marco Gestri and Gabriella Venturini (eds.) *International Disaster Response Law,* Springer, 2012, pp. 105-128.

Hahn, Johannes, European Commissioner for Regional Policy, "EU Solidarity Fund: Commission proposes €14.6 million to support Slovenia, Croatia and Austria after floods disaster", News release, European Commission, 30 Apr 2013. http://ec.europa.eu/commission_2010-2014/hahn/headlines/news/detail/index_en.cfm?LAN=EN&id=696&lang=en

International Civil Defence Organisation. http://www.icdo.org

Institute of Civil Protection and Emergency Management (ICPEM). http://www.icpem.net/

Konstadinides, Theodore, "Civil Protection in Europe and the Lisbon 'solidarity clause': A genuine legal concept or a paper exercise", Juridiska fakulteten, Uppsala universitet, 2011.

LaFeber, Walter, *America, Russia, and the cold war, 1945-1996,* McGraw-Hill, New York, 1997.

Norfolk Civil Protection Volunteers. www.norfolkcivilprotection.org.uk**.**

Sangster, H., D.K. Chester and A.M. Duncan, "Human responses to historical eruptions of Etna (Sicily) from 1600 to present and their implications for present-day disaster planning", Conference Proceedings, EGU General Assembly 2012, held 22-27 April 2012 in Vienna, Austria, p. 8477.

Scottish Government, Safer Scotland, Ready Scotland, Preparing for and dealing with emergencies, Resilience Division. www.readyscotland.org/ready-government/resilience-division/.

Scottish Government, Safer Scotland, Ready Scotland, Preparing for and dealing with emergencies, Resilience Advisory Board. www.readyscotland.org/ready-government/resilience-advisory-board/

Scottish Government, Safer Scotland, Ready Scotland, Preparing for and dealing with emergencies, ScoRDS. www.readyscotland.org/ready-government/scords/

South Eastern Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP). http://www.unisdr.org/files/18135_seedrmapbrochure.pdf

UK Government, "Public safety and emergencies: What we're doing". http://www.gov.uk/government/topics/public-safety-and-emergencies

UK Government, Cabinet Office, "Preparation and planning for emergencies: responsibilities of responder agencies and others", 20 Feb 2013. http://www.cabinetoffice.gov.uk/content/civil-contingencies-act

UK Government, Cabinet Office, "COBRA meeting on fuel contingencies", 28 Mar 2012. www.gov.uk/government/news/cobra-meeting-on-fuel-contingencies

UK Government, Cabinet Office, "Resilience in society: infrastructure, communities and businesses", 20 Feb 2013. https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses#corporate-resilience-sme-resilience-strategy

UK Government, Cabinet Office, "Voluntary Sector Civil Protection Forum, 2012", 17 Feb 2013. www.gov.uk/government/publications/voluntary-sector-civil-protection-forum-2012

UK Government, Civil Contingencies Act 2004. http://www.legislation.gov.uk/ukpga/2004/36/contents

UK Government, Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005, No. 2042, Part 7, Reg. 40. http://www.legislation.gov.uk/uksi/2005/2042/regulation/40/made

UK Government, Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005, 14 Nov 2005. http://www.legislation.gov.uk/ssi/2005/494/contents/made

UK Government, "National recovery guidance, generic issues: social media", 4 Oct 2012.https://www.gov.uk/government/publications/national-recovery-guidance-generic-issues-social-media

2.1.8 Resilience in the banking sector

Professor Kirstie Ball, Open University

The financial crisis has foregrounded the resilience agenda in the global banking sector and clear statements about the meaning of resilience within banking have emerged. The current financial crisis began in the US financial markets. Excessive, risky sub-prime mortgage lending caused huge financial losses as customers defaulted on their mortgages. A "credit crunch" resulted as credit was less available due to banks having to absorb these losses. This rapidly spread around the world as banks

tried to recover their losses in global financial markets and by trading complex and high risk financial instruments such as "securitisations" or "derivatives". Many banks did not have the capital or enough liquid assets to get themselves out of trouble. One large investment bank, Lehman Brothers, collapsed. Throughout the world, the public sector had to step in with injections of cash into the banks (liquidity) which then exposed the taxpayer to the banks' losses. As a result, economic demand decreased and many countries entered into a recession. It was acknowledged by the banking sector, on a worldwide basis, that it needed to be more resilient to "shocks" such as the one experienced in the 2008 financial crisis.

Current thinking on resilience in banking is embodied in the Basel III recommendations, implemented through national banking supervisory bodies. Basel is a set of banking regulations created by the Bank for International Settlements (BIS), a group of representatives from the G20 countries. To date, there have been three adaptations of the Basel regulations, referred to as Basel I, Basel II, and Basel III. Basel III was formulated in direct response to the financial crisis. In order to draw up their regulations, the Basel Committee conducted studies of 263 banks in 23 countries and the Committee of European Banking Supervisors involved 230 banks from 21 European countries.[195] Its measures are now formally adopted by banking supervisors in most of the Basel committee countries: Australia, Belgium, Brazil, Canada, France, Germany, Hong Kong SAR, India, Italy, Japan, Korea, Luxembourg, Mexico, The Netherlands, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, UK, and at EU level.

Definitions: Resilience in the banking sector

Within the banking sector, resilience is referred to in two ways:

1. The sector's ability to absorb shocks and therefore prevent or limit the extent of the damage caused beyond the banking sector by those shocks. In effect, this means containing any financial crisis within the sector in a way in which customers, the taxpayer and governments do not have to absorb any resulting financial losses.
2. The sector's ability to prepare for absorbing shocks in future.[196]

Resilience of what?

Basel III and evidence from elsewhere argues that the banking system has a number of features which need to be reformed in order that banking as a whole be more resilient.[197] These features occur at a variety of analytical levels which appear to be embedded within one another. They are as follows:

---

[195] Gromova-Schneider, Anastasia, and Caroline Niziolek, "The Road to Basel III – Quantitative Impact Study, the Basel III Framework and Implementation in the EU", *Financial Stability Report*, Vol. 21, 2011, pp. 58 – 61.

[196] Basel Committee on Banking Supervision, *Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems*, Bank for International Settlements, Basel, 2011.

[197] Walker, G.A., "Basel III Market and Regulatory Compromise", *Journal of Banking Regulation*, Vol. 12, Issue 2, 2011, pp. 95 - 99.

1. Banking practices
2. Monitoring and reporting
3. International industry standards
4. Understanding the banking industry in context

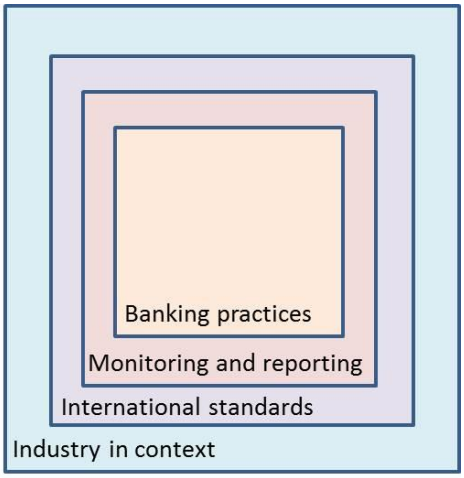

Figure 3 Features of the banking system

Increasing resilience in the first three levels relies, in no small part, on intensified surveillance of banks' internal features through the application of more exacting measures, disclosures and reporting requirements.

1. Resilience of banking practices

In the recent financial crisis, banks were unable to absorb the losses they incurred in their trading and lending activities. This was found to result from three interlinked issues:

- A lack of liquidity – easily accessible assets which could quickly mitigate losses.
- A lack of good quality capital – robust resources which could be used as collateral to mitigate the risks associated with trading and lending.
- Inadequate risk assessment associated with trading in overseas markets.

To increase resilience, banks were required to address these shortcomings. This was to be done in a number of ways. Banks were to:

1. Have better access to liquid assets and to set aside more of their capital for when times were hard. Up to 10.5% of total capital was to be set aside. This 10.5% was to comprise:
    a. 6% of 'tier1', or top quality, capital. This takes the form of share capital and disclosed reserves.
    b. 2% of 'tier2' capital (re-evaluation reserves, undisclosed reserves, hybrid instruments etc)
    c. Of this 8%, a minimum of 2.5% had to be conserved at all times, which was called the' 'capital conservation buffer'.
    d. In addition there is a discretionary 0% - 2.5% 'countercyclical buffer' which could be applied. The countercyclical buffer encourages banks

to save rather than spend when times are good, so that they have something left when times are lean.

2. Assess formally the risks associated with trading with other financial institutions in overseas markets. The risks were to be assessed on a per-asset basis, and using a ratio called the 'Risk-Weighted Assets' (RWA) banks had to show that they had enough capital to cover the risks associated with each asset they leveraged. They were subject to a charge if they made losses associated with a decline in the creditworthiness of a trading partner.
3. Use other suggested internal ratings based approaches to be implemented at the discretion of the national banking supervisor. For example, the use of credit ratings agencies and risk assessments of borrowers were considered.[198]

2. Monitoring and reporting on banking practices to increase resilience

As banks were required to change many of their internal practices, they were also expected to account for those changes and were subject to a number of new monitoring and financial reporting requirements. Little detail is given on how these issues will be reported or policed, however. One basic change was that all elements of capital held by a bank needed to be disclosed on their balance sheets. Prior to the financial crisis, this was not the case with all types of capital. Trading in the more complex financial instruments, such as over the counter derivatives, were not reported in any official documentation and so skewed the valuation of bank assets and their associated risks.

There were two specific reporting requirements related to liquidity and risk, which were directly aimed at increasing resilience:

a. The Liquidity Coverage Ratio (LCR), which explicitly addresses the issue of short term resilience. Banks were required to show that they had enough high quality liquid resources to survive an acute stress for a month.
b. Net Stable Funding Ratio (NSFR), which explicitly addresses what in banking terms is considered "long term" resilience. It encourages banks to maintain a long-term, stable, funding base (for example, through customer long-term deposits or money borrowed from a stable central fund) for a period of one year and not to trade on them in the short term. "Encouragement" in this context indicates a reporting requirement. Banks had to determine the minimum acceptable amount of long-term funding that was needed in relation to the relative risks of the liabilities in which they had invested. This was seen as something that had the potential to reverse the fortunes of the banking sector.[199]

National banking supervisors were also encouraged to consider a number of other measures to help predict where liquidity problems might occur. A number of metrics were suggested:

---

[198] Basel Committee on Banking Supervision, *Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems*, Bank for International Settlements, Basel, 2011.
[199] Bernstein Black Book, "Game Changer: Basel III's Impact on Bank Profitability and Capital Return", June 2012, pp. 1 - 117.

a. Contractual maturity mismatch: where banks conduct an analysis of their contractual commitments to identify where they will need quick access to liquid assets.
b. Concentration of funding: where supervisory authorities analyse concentrations of large-scale funding provided by particular trading partners, instruments and currencies. This indicates areas where liquidity crises could occur if any one of the funding sources are withdrawn.
c. Available unencumbered assets: this metric measures the amount of assets a bank has which could potentially be used as collateral for secured funding in the market or at a central bank. This could make banks aware of their capacity to raise additional unsecured funds if they need to do so, for example, in an emergency.
d. Market-related monitoring tools: to have instantaneous data on monitoring activities, get market-wide data on asset prices and liquidity, institutional information such as its availability to swap credit defaults and its ability to fund itself in wholesale funding markets.

Since the publication of Basel III, different countries around the world have debated how they would implement these and other measures deemed appropriate for their economic contexts. Many post-Basel academic publications have concerned the most appropriate ratios.[200] Central and Eastern European countries have been particularly vocal in this regard. They have relied on credit expansion for growth during times of economic boom. As a result, they are not sure that the countercyclical buffer is appropriate for when they have a buoyant economy. They argue that it will hold back growth and make their overall economies perhaps less resilient.[201]

A further concern is that these changes will result in higher costs for banks which will negatively affect their long term competitiveness.[202] Within banks, significant strategic resources will need to be invested in building an integrated vision for the management of credit risk and default in trading. Financial trading, at best, is an opaque practice and rendering it accountable is difficult and controversial. Methodologies will need to be developed for calculating risks, high-quality, reliable data will need to be gathered and effective internal governance mechanisms will need to be put in place.[203]

3. System-wide resilience measures

[200] Dardac, Nicolae, and Alina Grigori, "Modeling the Market Risk in the Context of the Basel III Accord", *Theoretical and Applied Economics*, Vol. 18, Issue 11, 2011, pp. 5 - 20; Dedu, Vasile, and Dan Costin Nitescu "Basel III – Between Global Thinking and Local Acting", *Theoretical and Applied Economics*, Vol. 19, Issue 6, 2012, pp. 5 – 12; Rossignolo, Adrián, Meryem Duygun Fethi and Mohamed Shaban, "Market Crises and Basel Capital Requirements: Could Basel III Have Been Different? Evidence from Portugal, Ireland, Greece and Spain", *Journal of Banking and Finance*, Vol. 37, Issue 5, 2013, pp. 1323 – 1339.
[201] Geršl, Adam, and Jakub Seidler, "Excessive Credit Growth and Countercyclical Capital Buffers in Basel III: An Empirical Evidence from Central and East European Countries", *Economic Studies and Analysis*, Vol. 6, Issue 2, 2012, pp. 91 – 107.
[202] PriceWaterhouseCoopers, "PwC Highlights Gaps in Basel III Draft", *Financial Management*, October 2010, pp. 6 – 6.
[203] Nucu, A. E., "The Challenges of Basel III for the Romanian Banking System", *Theoretical and Applied Economics*, Vol. 18, Issue 12, 2011, pp. 59 – 70.

Although the lion's share of these new regulations was aimed at banking practices and their national governance, Basel III has sought international harmonisation of resilience measures in its focal key areas of liquidity management and risk assessment. Regarding liquidity, both the Liquidity Coverage Ratio and the Net Stable Funding Ratio are to be harmonised internationally into a "Global Minimum Liquidity Standard". As far as risk management is concerned, an internationally harmonised "Leverage Ratio" is to be developed. Leverage occurs is when banks borrow more to increase the return on an investment. Effectively, they borrow to make the amount they invest larger and therefore to increase the return. An international leverage ratio would assess the ratio of overall debt to equity with the intention of restraining debt to an internationally agreed level when it grew too large. By comparison, for national governments this is typically assessed by expressing national debt as a percentage of gross domestic product (GDP).

4. The banking sector in context

Critics of Basel III are keen to point out that it focuses too much on the banking practices without addressing structural issues within the sector which also impact its resilience in times of stress. External monitoring of the bank system as a whole as well as improved national and international enforcement mechanisms for Basel III have been called for.[204] Structural issues which remain to be addressed concern:

a. Bank business models which allow financial cross fertilisation between the retail and investment arms of individual banks. Separating the retail and investment divisions of banks will prevent investment losses impacting consumer products. Bank regulations in different jurisdictions have addressed this but it is not a universal measure. For example, the Dodd–Frank Wall Street Reform and Consumer Protection Act, adopted in the US in July 2010, introduces restrictions on bank diversification. Similarly, in the UK, the Independent Commission on Banking, established in June 2010, suggests the creation of ring-fenced banks which have to focus, exclusively, on retail banking and have to be legally separated from other entities when they belong to a financial group.[205]

b. Overall bank size, or the 'too big to fail' argument. Some commentators have argued that Basel III would be more effective if there was an absolute cap on bank size in relation to the economy wherein it is located[206].

[204] Vassiliadis, Spyros, Diogenis Baboukardos and Panagiotis Kotsovolos, "Is Basel III a Panacea? Lessons from the Greek Sovereign Financial Crisis" *South East European Journal of Economics and Business* Vol. 7, Issue 1, 2012, pp. 73 - 80

[205] Vallascas, Francesco and Kevin Keasey "Bank Resilience to Systemic Shocks and the Stability of Banking Systems: Small is Beautiful" *Journal of International Money and Finance* Vol. 31, 2012, pp 1745 – 1776.

[206] Vallascas, Francesco, and Kevin Keasey, "Bank Resilience to Systemic Shocks and the Stability of Banking Systems: Small is Beautiful", *Journal of International Money and Finance*, Vol. 31, 2012, pp. 1745 – 1776.

Conclusion

Although little has been written on resilience in the banking sector per-se, the current financial crisis has produced insight into how the concept of resilience has become mobilised within the sector. Overall, resilience is referred to as the capacity to absorb shocks and in terms of capacity building to contain the effects of those shocks in future. Resilience is operationalised at multiple levels of the banking sector, focusing on setting standards for liquidity management, capital buffers and risk assessment within the internal workings of banks. These three features of banking operations were deemed to render banks most vulnerable to sudden and unexpected financial losses. A stringent set of reporting requirements enforce these standards at national level and there are aspirations for the international harmonisation of key measures. Local variation is expected in the implementation of Basel III but there are still issues around the external monitoring of the banking sector as a whole.

References

Basel Committee on Banking Supervision, *Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems*, Bank for International Settlements, Basel, 2011.

Bernstein Black Book, "Game Changer: Basel III's Impact on Bank Profitability and Capital Return", June 2012, pp. 1 - 117.

Dardac, Nicolae, and Alina Grigori, "Modeling the Market Risk in the Context of the Basel III Accord", *Theoretical and Applied Economics*, Vol. 18, Issue 11, 2011, pp. 5 – 20.

Dedu, Vasile, and Dan Costin Nitescu, "Basel III – Between Global Thinking and Local Acting", *Theoretical and Applied Economics*, Vol. 19, Issue 6, 2012, pp. 5 – 12.

Geršl, Adam, and Jakub Seidler, "Excessive Credit Growth and Countercyclical Capital Buffers in Basel III: An Empirical Evidence from Central and East European Countries", *Economic Studies and Analysis*, Vol. 6, Issue 2, 2012, pp. 91 – 107.

Gromova-Schneider, Anastasia, and Caroline Niziolek, "The Road to Basel III – Quantitative Impact Study, the Basel III Framework and Implementation in the EU", *Financial Stability Report*, Vol. 21, 2011, pp. 58 – 61.

Nucu, A. E., "The Challenges of Basel III for the Romanian Banking System", *Theoretical and Applied Economics*, Vol. 18, Issue 12, 2011, pp. 59 – 70.

Rossignolo, Adrián, Meryem Duygun Fethi and Mohamed Shaban, "Market Crises and Basel Capital Requirements: Could Basel III Have Been Different? Evidence from Portugal, Ireland, Greece and Spain", *Journal of Banking and Finance*, Vol. 37, Issue 5, 2013, pp. 1323 – 1339.

Vassiliadis, Spyros, Diogenis Baboukardos and Panagiotis Kotsovolos, "Is Basel III a Panacea? Lessons from the Greek Sovereign Financial Crisis", *South East European Journal of Economics and Business*, Vol. 7, Issue 1, 2012, pp. 73 – 80.

Vallascas, Francesco, and Kevin Keasey, "Bank Resilience to Systemic Shocks and the Stability of Banking Systems: Small is Beautiful", *Journal of International Money and Finance*, Vol. 31, 2012, pp. 1745 – 1776.

Walker, G.A., "Basel III Market and Regulatory Compromise", *Journal of Banking Regulation*, Vol. 12, Issue 2, 2011, pp. 95 – 99.

2.1.9 Critical infrastructures: Resilience and telecommunications networks

Dr Nils Zurawski, University of Hamburg

The threat of breakdown in regional and global communications is omnipresent in media publications and official documents on telecommunication infrastructure throughout the world.[207] Breakdowns can occur because of an overload of traffic on a given network, be it mobile or cable; attacks on the infrastructure – as happened in Egypt in March 2013 when attacks on telecom sea cables were attempted; technological failures or problems, such as the exhaustion of Internet addresses in the old IP 4 protocol. It is estimated that 95 per cent of all global telephone communications rely on sea or land cables and only 5 per cent is relayed by satellites,[208] hence, the importance of this infrastructure becomes self-evident. Resilience of this infrastructure on different levels thus constitutes a major concern for many parties involved.

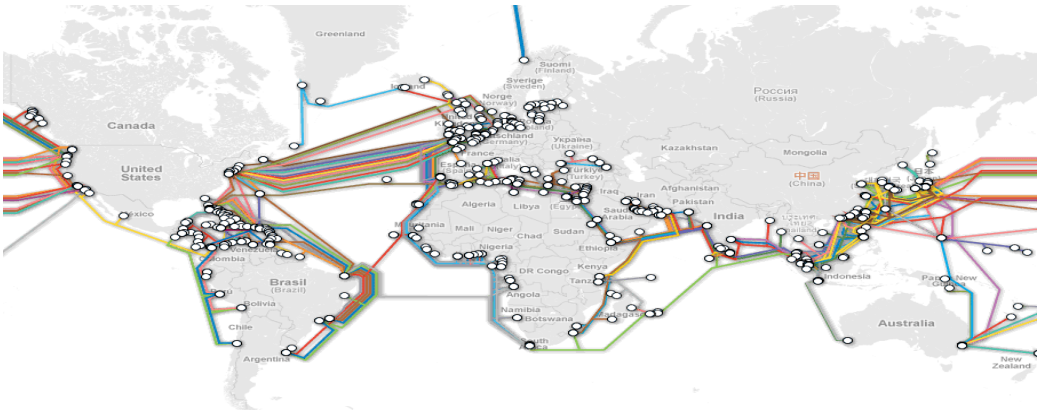

Figure 4 Submarine cable map[209]

How is the term 'resilience' used and defined?

[207] See http://www.golem.de/news/sabotage-kriminelle-haben-internet-seekabel-durchschnitten-1303-98436.html; http://www.welt.de/wirtschaft/webwelt/article12510752/Deutschland-steht-vor-riesigem-Mobilfunk-Crash.html; http://www.handelsblatt.com/technologie/it-tk/special-cloud-computing/industrie-warnt-cloud-computing-belastungsprobe-fuer-das-netz/4005500.html; http://www.ewi.info/reliability-global-undersea-communications-cable-infrastructure; Conrad, David, "Towards Improving DNS Security, Stability, and Resiliency", Internet Society, 2012. http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

[208] Matis, Michael, "The Protection of Undersea Cables: A Global Security Threat", United States Navy, 2012. https://www.hsdl.org/?view&did=718794

[209] TeleGeography. http://www.submarinecablemap.com/

Defining the concept of resilience in other domains may be more difficult, but in the case of telecommunications, there is some clarity and unity about how the term is understood. The Wikipedia entry defines telecoms resilience as follows:

> The term telecoms resilience means enabling a telephone subscriber to continue to be served even when one line is out of service. The UK carrier networks are required by Ofcom to be 99.999% resilient. This means there should be no more than 5 minutes per year downtime in any single telephone exchange.[210]

US national security has a similar definition and views resilience as the capability of a system to maintain its functions in the face of internal and external events.[211] This definition is consistent with that of the Critical Infrastructure Task Force (Homeland Security Advisory Council, 2006) and the National Strategy for Homeland Security (Homeland Security Council, 2007).

The European Network and Information Security Agency (ENISA) report conceptualises resilience thus:

> ENISA has defined resilience as "the ability of a system to provide & maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation." This can be contrasted with a definition of resilience where stress is applied to the system, "The ability of an entity, system, network or service to resist the effects of a disruptive event, or to recover from the effects of a disruptive event to a normal or near-normal state". The former does not address stress and recovery and may be considered as closer to reliability and thus using this as the definition for this report could lead to a focus on an inappropriate set of measures to give assurance of resilience. Reliability is addressed in the security domain by the Availability parts of the CIA paradigm and by existing Quality of Service (QoS) and Grade of Service (GoS) metrics. Therefore, it is important to distinguish resilience, and the means to design for resilience, from the techniques and technologies to achieve reliability. [212]

It is interesting to note here that a distinction is made between reliability and resilience. The report goes on to feature yet another definition, which sees resilience as:

> Resilience is the aptitude of an organisation to keep its systems and services running under an emergency situation, to maintain the highest possible level of performance, to resume a nominal mode of functioning as quickly and easily as possible should

---

[210] Wikipedia, "Telecoms Resilience". http://en.wikipedia.org/wiki/Telecoms_resilience; See also Centre for the Protection of the National Infrastructure (CPNI) 2006, Telecommunication Resilience. Good Practice Guide, March 2006. Version 4, https://www.cpni.gov.uk/documents/publications/undated_pubs/1001002-guide_to_telecomms_resilience_v4.pdf

[211] Crain, John K., "Assessing Resilience in the Global Undersea Cable Infrastructure", Master thesis, Naval postgraduate school, Monterey California, June 2012. http://calhoun.nps.edu/public/handle/10945/7327

[212] ENISA, "Enabling and managing end-to-end resilience". http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/e2eres

> performance have decreased, and to draw the lessons from the experience once the crisis is over.[213]

Interestingly, the report's definition closes by saying that "Resilience management is a learnt and prepared aptitude. It cannot be improvised at incident response time." Failures of the system, to which the ENISA report is referring to, have been addressed elsewhere, especially when concerning the sea cables or the other parts of the vital infrastructure. The International Telecommunication Union (ITU), for instance, has identified this as a vital issue. The Internet Society has addressed this issue in regard to the stability and resilience of the Domain Name System (DNS), as has ENISA with regard to Internet interconnection.

Booz Allen Hamilton's report for the Economist Intelligence Unit, highlights Nigel Inkster's (Director of Transnational Threats and Political Risk at the International Institute for Strategic Studies) definition of cyber resilience, "the ability of a system or domain to withstand attacks or failures, and in such events, to re-establish itself quickly".[214]

However, in discussing the concept, this report too stresses the fact that there is some tension between the concept of "reliability" and "availability". It highlights that a new attitude in achieving resilience is to plan for "acceptable" levels of data loss, unit failures and compromise. But, new cloud hardware architectures are demonstrating that everyday events like storage device failures and data loss can be tolerated when redundancies are built into the system. When everything is critical, nothing is critical. Such a perspective has also been taken when defining DNS resiliency in a report by the Internet society:

> The ability of the DNS to provide and maintain an acceptable level of name resolution service in the face of faults and challenges to normal operations.[215]

In short, resilience in the field of telecommunications is used to secure the infrastructures of communications in the case of a breakdown. This implies preparedness for adverse events, "natural" hazards or other failures, such as overloads. Resilience does not necessarily ensuring a 100 per cent performance; rather it means providing an available system in order to be able to communicate even in the case of an attack or other emergency circumstances.

Rationale and justifications for using the concept

The main rationale or argument for using the concept, given the only slightly varying definitions, is the pivotal importance of telecommunications for almost all aspects of political, social and economic life in today's world. At a closer glance, this rationale presents two aspects.

- Telecommunications is of utmost importance in cases of emergency, to co-ordinate help, to uphold social order and to secure flows of data, which are

[213] Ibid.
[214] Booz Allen Hamilton, "Resilience in the Cyber Era: Building An Infrastructure that Secures and Protects". 2011. http://www.boozallen.com/media/file/resilience-in-the-cyber-era.pdf
[215] Conrad, David, "Towards Improving DNS Security, Stability, and Resiliency", Internet Society, 2012. http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

important for the global economy. Telecommunication is a major backbone of many forms and strategies of resilience in cases of adverse events, "natural" hazards or social upheaval. In the latter case, it may become a source for active resistance as well. Network shutdown in Egypt during the Arab spring may be an indication of this.

- Therefore, it is necessary to guarantee network resilience, i.e., to make sure at least some lines remain in place to counter adverse events such as those mentioned above.

Examples:

Economic rationale: "Increased harmonization of submarine telecommunication cable protection ensures seamless internet connectivity across the Asia-Pacific's fast-growing web-based economies," says a report commissioned by the Asia-Pacific Economic Cooperation (APEC) Policy Support Unit.[216]

Political rationale: Europe is well aware of the economic chaos and social disorder that could result from the breakdown of its information and telecommunications infrastructure, due to an attack, technical failure or natural disaster. "Preparedness, or the ability to respond effectively to this type of crisis, calls for the coordinated mobilisation of many different stakeholders at government level and industry, public sector and private, as well as a common culture of security."[217]
A *military rationale* would make use of the former two, turning their interests into national ones. The functioning of the state before all other is of prime concern here.[218]

Disaster rationale: "Recent events have clearly demonstrated the need for telecommunications networks to be resilient to natural and human-induced disasters, as they are critical to rescue efforts and restoring normality in the wake of disasters."[219]

Characteristics or features of the concept

The key features of the concept circle around the aspects of the integrity of the infrastructure on one side, and the availability of various services on the other. The latter would include Internet services, as in the case of DNS security and resilience, as well as the physical integrity of sea (and other) cables. There have to be "enough" lines and capacity to deal with all communications arising at one particular point in

[216] APEC Committee on Trade and Investment, "APEC: Submarine cable resilience critical to connectivity", Press release, Jakarta, Indonesia, 6 Feb 2013. http://www.apec.org/Press/News-Releases/2013/0206_cable.aspx

[217] Thales, "Enhancing European Resilience". http://www.thalesgroup.com/News_and_Events/Markets/Security/230310_Focus_Enhancing_European_resilience/. See also the blog: Sicherheits-Politik: http://www.sicherheitspolitik-blog.de/2012/11/06/drohnen-und-swift-unter-wasser/

[218] Crane, op. cit., 2012; see also Sicherheits-Politik: http://www.sicherheitspolitik-blog.de/2012/11/06/drohnen-und-swift-unter-wasser/

[219] The Assembly, "Telecommunications crucial when disaster strikes", *Blog of the World Telecommunication Standardization Assembly*, 23 Nov 2012. http://wtsa12.wordpress.com/tag/resilience/

time – so the amount and strength of the system is vital; these lines have to be in good state and must be secured and defended – as a military rationale would claim.

The following initiatives and official bodies provide examples of the measures through which the concept is implemented in different areas:

- ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery (FG-DR&NRR)[220]
- ENISA Critical Information Infrastructure Protection (CIIP) and Resilience Unit.[221]

Both initiatives focus on development and education in relation to security issues regarding telecommunications infrastructures. Both serve as co-ordinating and standards-setting agencies to ensure a wide distribution of measures and the implementation thereof. Resilience in both cases has to do with the generation of structures that can be relied upon in a case of emergency. The agencies want to ensure everything is "ready" and in place when a failure or disaster happens. Their overall aim is to harmonise national concepts to a common standard. Therefore, the working groups, or initiatives, facilitate communication to foster the establishment of standards for relief communication and security measurements in the case of an emergency:

> The catalyst behind creating this focus group dates from the end of last year when we had a couple of requests from the Chief Technology Officers from KDDI and NTT in Japan. They had lived through the earthquake and subsequent tsunami and from that experience they realised that although there are already standards and techniques for disaster relief and network resilience but they are not sufficient from the experience that they had in Japan.[222]

Policy aspects and/or strategic aspects of resilience

Resilience in telecoms infrastructures mainly involves planning ahead, i.e. in the instance of telecoms networks, planning for breakdowns as well as building in redundancy is paramount. The main actors together with the national telcos are involved in setting standards for performance, regulations and procedures for cases of emergencies (e.g., at the level of ITU; ENISA, European Union and other bodies) Given that there is a clear number of actors involved, this seems a viable option and strategy. Lessons learned from previous breakdowns will be built in future resilience strategies. Telecoms resilience focusses distinctively on infrastructure and the technology. Scenarios beyond this, i.e. the general public or political consequences are not the prime interest. More or less, resilience in the case of telecom infrastructures is all about preparedness and anticipation - technical, organisational and in military terms.

Lessons from an IRISS perspective

---

[220] ITU. http://www.itu.int/en/ITU-T/focusgroups/drnrr/Pages/default.aspx
[221] ENISA, "Resilience and CIIP". http://www.enisa.europa.eu/activities/Resilience-and-CIIP
[222] Jamoussi, Bilel, Chief, Study Groups Department, ITU Telecommunication Standardisation Bureau, "Interview on the establishment of the focus group FG-DR&NRR", *Intercomms*, Issue 18, May 2012. http://www.intercomms.net/issue-18/dev-1.html

If we take surveillance as a term that implies monitoring something, then resilience strategies in relation to telecommunication means to watch lines and infrastructure closely to avoid breakdowns or to minimise the negative effects of failures. However, there does not seem to be a direct connection between the employing such strategies and a surveillance society (whatever that might be and in whatever disguise it comes along). But there are a few points that may be interesting to explore further as telecommunication lies at the heart of much modern day surveillance and control strategies, most of all those that have to do with digital data collection.

- Cyber resilience or DNS security seems to imply the monitoring of online activities to avoid breakdowns or attacks on the system. Hence, resilience could be achieved by a heightened proactive control.
- Network analyses of the problem of infrastructure resilience suggest that cables are a weak point as there are too many to secure all of them. To avoid breakdowns means to be prepared and develop alternative solutions, especially for emergencies.
- Paying more attention to future assaults on sea cables would mean a new focus for proactive surveillance of other forms of communications to deter or intercept planned attacks.
- The main strength of resilience strategies in this field is based on standardisation across national boundaries. Resilience would then follow common procedures and communications could be diverted or substituted worldwide. However, in other cases of resilience, this model may not be the best idea, as it does not pay attention to local specificities. In the case of telecoms resilience, this is not so necessary; in other areas of social and political life, this may well be necessary for the survival of a society.

2.2 HORIZONTAL ANALYSIS OF HOW THE TERM "RESILIENCE" IS USED ACROSS DIFFERENT DOMAINS

This section consists of a horizontal (or comparative) analysis of how "resilience" is used terminologically, conceptually, strategically and politically across the different domains discussed in section 2.1. In section 2.1, we analysed the use of the term in nine different domains, i.e., those of the European Commission, the UK Cabinet Office, dictatorial and post-dictatorial regimes, US cyber security, the United Nations, public transport, civil protection, banking and critical infrastructure (i.e. telecoms networks). The three main purposes of this horizontal analysis are, first, to identify the commonalities and differences in the way the term "resilience" is used; second, to help us characterise "resilience" in the face of pervasive surveillance in a democratic society; and third, to set out some propositions regarding resilience in a surveillance society based on the findings of this section.

2.2.1 Definitions of resilience – commonalities and differences

Resilience has been defined in different ways, as the following examples indicate:

The European Commission (EC) Communication on the EU Approach to Resilience defines resilience as "the ability of an individual, a household, a community, a

country or a region to withstand, to adapt, and to quickly recover from stresses and shocks".[223] This definition would work in any discussion of resilience in the context of a surveillance society.

The UK Cabinet Office defines resilience somewhat similarly: "The capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure, and identity".[224] Resilience is also defined as "The ability of a system or organisation to withstand and recover from adversity."[225] This definition would also serve any discussion of resilience in the context of surveillance societies. "Community resilience" is defined as "Communities and individuals harnessing local resources and expertise to help themselves in an emergency, in a way that complements the response of the emergency services."[226] This definition is rather more focused on emergencies and disasters and civil protection. One might say this definition ignores the ability of communities to be resilient even in the absence of the emergency services. The UK Cabinet Office itself uses the term in some different ways. For example, in the context of cyber security, the term "resilience" is used in the sense of offering "protection" from possible cyberattacks; "resilience" is also used in the sense of "business continuity" (meaning having the capability to provide uninterrupted services, or at least to minimise server downtime). The UK Cabinet Office uses the notion of "resilience" almost exclusively in relation to security, health, disaster or other threats; it is not used in relation to "resilience" to or against challenges to democratic society that might be posed by surveillance or security measures.

The extent and power of surveillance, today, are far greater than state surveillance highlighted in Central and Eastern Europe in the bad old days of the communist era. In some situations, as section 2.1.3 highlights, the notion of resilience is difficult to interpret in a transitional period when the points of reference themselves are on the move. In the face of the political revolutions that took place in Eastern Europe in the late 1980s, some countries such as Czechoslovakia and Hungary retained their legal and administrative frameworks throughout the whole process of transitioning from communist to democratic societies. We can attribute to them a sort of *structural resilience*, in contrast to those countries where the collapse of the old regime was accompanied by the abolition of laws and institutions, bloodshed and even executions, as was the case in Romania.

In some domains, such as national security, the term "resilience" is widely used and differently defined. The most extensive definition is provided in the US *Presidential Policy Directive – Critical Infrastructure Security and Resilience* which defines it as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from

[223] European Commission, 2012, op. cit. p. 7.
[224] Cabinet Office, *Strategic National Framework on Community Resilience*, London, Cabinet Office, 2011, p. 4. The original source of the definition is given as Charlie Edwards, *Resilient Nation*, London, Demos, 2009. http://www.demos.co.uk/files/Resilient_Nation_-_web-1.pdf
[225] Cabinet Office, *Strategic National Framework,* op. cit., 2011, p. 10.
[226] Cabinet Office, *Strategic National Framework,* op. cit., 2011, p. 4. The definition is drawn from an earlier Cabinet Office resource.

deliberate attacks, accidents, or naturally occurring threats or incidents."[227] This definition would also serve any discussion of resilience in a surveillance society.

The Glossary of the US Office of Infrastructure Protection Strategic Plan defines resilience more succinctly as the "ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions".[228] This one too would serve in any discussion of resilience in a surveillance society. The second US National Strategy for Homeland Security, published in 2007, uses the terms "resilience" and "resilient" frequently, especially in the context of critical infrastructure protection[229] and key assets that permit the building of "a more resilient Nation".[230] The document also introduces the notion of "operational resilience", which refers to ensuring organisational continuity in case of disaster.[231] This definition is too narrow to serve in a discussion of resilience in a surveillance society. It is more applicable to the resilience of critical infrastructure. The 2012 US Department of Homeland Security (DHS) Strategic Plan[232] generalises the term "resilience": not only is it used in relation to critical infrastructure protection,[233] it is also used in relation to the "nation" and "homeland", and in particular to "disasters".[234]

US security documents indicate that resilience is not only regarded as mere bouncing back or survival, but also an occasion to grow stronger after adversity. This thought would serve our aforementioned discussion, especially if we interpret it to mean an occasion for individuals, groups and society as a whole to grow stronger in the face of adversity, i.e., specifically the challenges to fundamental rights posed by many forms of surveillance. The 2010 National Security Strategy states that "national security draws on the strength and resilience of our citizens, communities, and economy".[235] The DHS Strategic Plan for the period 2012-2016 uses the term not only in reference to material infrastructures or information systems, but also in reference to "global movement systems", "key nodes of transaction and exchange within the global supply chain", "maritime transportation systems" and "communities"; indeed, the entire "Nation".[236] Resilience implies a rallying together of a wider group of actors, sharing both forces and responsibilities for the continuous preparation against adverse events

[227] The White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience", The White House, Washington, DC, 2013.
[228] Office of Infrastructure Protection, "Office of Infrastructure Protection Strategic Plan: 2012-2016", Department of Homeland Security, Washington, DC, 2012, p. 14, emphasis in original.
[229] Homeland Security Council, op. cit., 2007.
[230] "By protecting CI/KR, we further protect the American people and build a safer, more secure, and more resilient Nation"; ibid., p. 25
[231] Ibid., p. 29
[232] Department of Homeland Security, "Department of Homeland Security Strategic Plan. Fiscal Years 2012-2016", Department of Homeland Security, Washington, DC, 2012.
[233] Cf. "Objective 1.3.3: Make critical infrastructure resilient"; ibid., 5
[234] For example, the main mission of the DHS is defined as follows: "We will lead efforts to achieve a safe, secure, and **resilient homeland**. We will counter terrorism and enhance our security; secure and manage our borders; enforce and administer our immigration laws; protect cyber networks and critical infrastructure; and ensure **resilience from disasters**"; [Department of Homeland Security, 2012 #10@ 2, emphasis added]
[235] The White House, "National Security Strategy", 2010, p.10.
[236] Department of Homeland Security, "Department of Homeland Security Strategic Plan. Fiscal Years 2012-2016", 2012.

and punctual mobilisation in case of disruption. Rallying together would be an appropriate feature of resilience in a surveillance society.

In UN documents, resilience is generally seen as an aspect of adaptation, and thus as "the ability to cope with climate change and natural disasters, in particular those associated with droughts, sea-level rise, increased temperatures and extreme weather events".[237] Resilience in this sense is not so relevant to a discussion of resilience in a surveillance society. Elsewhere, resilience is associated with social protection, disaster risk reduction, the ability to deal with stress and shocks, precautionary strategies to prevent adverse impacts, and "resilience planning".[238] In the same general area of global concern, the UN's Food and Agriculture Organization (FAO) highlights the need for strategies and policies to increase resilience to drought, with an emphasis on prevention and proactive drought management in the face of climate change, but it invokes no general definition.[239] Again, this use of resilience in not applicable to our discussion.

The UN International Strategy for Disaster Reduction (UNISDR) defines resilience as "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions." [240] Again, this definition of resilience is not applicable to our discussion. The disasters in focus here are "predictable" weather and weather-related events (e.g., floods), as well as earthquakes and tsunamis.

The terms "resilience" and "resilient" are used profusely as normative and empirical language in many UN documents, although in others their relevance and meaning are matters of inference and interpretation. To be resilient is regarded as desirable; becoming resilient is regarded as an important policy objective. Obstacles to resilience are seen as problems to be tackled, overcome or worked around. Resilience is life-affirming; lack of resilience results in disaster or death, or in the violation of human rights and freedoms. Not being resilient is a misfortune that can be righted through the application of analysis and resources of many kinds. However, these terms – "resilience" and "resilient" – are often not defined, their attributes are often left without explanation, and their relationship to adverse events and the effect of these events on people is often ambiguous.

---

[237] Ibid., para. 134.
[238] Ibid., paras. 136-138.
[239] Food and Agriculture Organization, "UN lays foundations for more drought resilient societies: Meeting urges disaster risk reduction instead of crisis management", 15 March 2013. http://www.fao.org/news/story/tr/item/172030/icode/en/
[240] UN System Task Team on the Post-2015 UN Development Agenda, *Disaster risk and resilience – Thematic Think Piece*, May 2012, p. 3, note 1. http://www.un.org/millenniumgoals/pdf/Think%20Pieces/3_disaster_risk_resilience.pdf. The definition is from United Nations Office for Disaster Risk Reduction, *UNISDR Terminology and Disaster Risk Reduction*, Geneva, UNISDR, 2009, p. 24. http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf. The UNISDR's comment on this definition is: "Resilience means the ability to 'resile from' or 'spring back from' a shock. The resilience of a community in respect to potential hazard events is determined by the degree to which the community has the necessary resources and is capable of organizing itself both prior to and during times of need."

In the UN's World Health Organization's (WHO) manual on dealing with mental health, intended as a popular guide, "resilience" is defined as "the capacity to manage oneself when faced with difficult circumstances, to transform oneself in a positive way, and to recover from the distressful event and survive".[241] This definition might have some relevance to our discussion where, for example, we could consider the impacts on fundamental rights caused by surveillance as the "difficult circumstances" and the "distressful event". But resilience in a surveillance society is only somewhat marginally focused on "managing oneself" in a surveillance society. Our focus is not so much focused on managing oneself as it is on developing techniques for living in a surveillance society.

Within the banking sector, resilience is referred to in two ways: First, it refers to the sector's ability to absorb shocks and therefore prevent or limit the extent of the damage caused beyond the banking sector by those shocks. In effect, this means containing any financial crisis within the sector in a way in which customers, the taxpayer and governments do not have to absorb any resulting financial losses. Second, it refers to the sector's ability to prepare for absorbing shocks in future.[242] This definition of resilience is too sector-specific to serve our discussion. However, there are certain features from the financial sector's use of the term "resilience" we can adopt for our discussion of resilience in a surveillance society, i.e., risk management, accountability and perhaps even harmonisation of resilience measures internationally.

The Wikipedia entry defines "telecoms resilience" as "enabling a telephone subscriber to continue to be served even when one line is out of service".[243] The European Network and Information Security Agency (ENISA) defines resilience as the ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional or naturally caused) affecting normal operation.[244] ENISA says that resilience has also been defined as "the aptitude of an organisation to keep its systems and services running under an emergency situation, to maintain the highest possible level of performance, to resume a nominal mode of functioning as quickly and easily as possible should performance have decreased, and to draw the lessons from the experience once the crisis is over".[245] These definitions are applicable to the resilience of a physical communications network, but less applicable to our discussion of resilience in a surveillance society. These definitions of resilience are closer to "reliability". Using such reliability definitions for this report would be misleading, inappropriate and defocus from the key issue of how we should live our lives and what we should do about the pervasiveness of surveillance in today's society. One can and should distinguish reliability from resilience.

Before moving on, it is interesting to note that ENISA says that "[r]esilience management is a learnt and prepared aptitude. It cannot be improvised at incident

---

[241] Ibid.
[242] Basel Committee on Banking Supervision, *Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems* Bank for International Settlements, Basel, 2011.
[243] http://en.wikipedia.org/wiki/Telecoms_resilience; also CPNI 2006
[244] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/e2eres
[245] ENISA, *Enabling and managing end-to-end resilience*, Heraklion, 24 Jan 2011, p. 9. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/e2eres

response time."[246] This point could be included in a discussion of resilience in a surveillance society.

The 2010 US National Security Strategy defines resilience as "the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption". This definition is somewhat similar to that of the EC, the first cited in this section. A very similar definition is also proposed in the Glossary of the Office of Infrastructure Protection Strategic Plan: "Resilience: ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions". This definition introduces two quite interesting differences: the first concerns the introduction of the adverb "successfully", and the second the pairing of a somehow more neutral "change in conditions" to "adversity" (instead of disruptions, attacks, accidents, incidents or threats). These small differences open the idea of resilience not only as mere bouncing back or survival, but also as an occasion to grow stronger after adversity. This indicates the prospect of some modification of structure, culture and/or behaviour in order to deal better with the future. This could be important in the case of resilience to surveillance.

The 2007 National Strategy for Homeland Security identifies two main types of resilience: "structural" and "operational".[247] Structural resilience can be defined as the "the ability of power, communications, and other life sustaining systems to survive an attack by terrorists, a natural disaster, and other assessed risks or hazards".[248] The definition of operational resilience is more interesting, as it considers the government itself as a sort of critical infrastructure.

All these documents mention resilience in relation to the infrastructures, the networks or the information systems, and often as a condition that is not yet fully achieved. Even the very premise of the 2009 Cyberspace Policy Review is highlighted as being extremely programmatic (see section 2.1.4).

In sum, the analysis shows commonalities and differences in the definition and use of the term "resilience". In some instances, it refers to an ability to adapt to situations in which stresses and/or shocks or adverse events are experienced. In network security, resilience refers to the ability and capacity to maintain an acceptable grade of service. In natural disasters, resilience means the ability of people to recover from shocks, such as storms, droughts, floods, earthquakes, fires, etc. Some of the above definitions of resilience (e.g., that of the EC) are satisfactory and usable for defining resilience in a surveillance society. However, we could provisionally define rather more specifically "resilience in a surveillance society" (the subject of the IRISS project) as **the ability of people (individuals and groups) and organisations to adapt to and/or resist surveillance, while recognising that some forms of surveillance may be acceptable or tolerable, while others pose a serious challenge to our fundamental rights.**

2.2.2 Role of surveillance in the analysed domains

[246] Ibid., p. 10.
[247] Homeland Security Council, "National Strategy for Homeland Security", The White House, Washington, DC, 2007.
[248] Ibid., p. 28

The role of surveillance in the analysed domains is not straightforward to determine. In some cases it is clear that surveillance forms an essential part of, and underpins resilience strategies. It is seen as a tool or mechanism that facilitates or achieves resilience. This is clearly illustrated in the cases of European Commission, US cyber security and critical infrastructure protection policies and the analysis of the public transport systems. Many of the strategic documents in these fields propose policies that foster, implicitly or explicitly, surveillance measures. Even the resilience of communities is perceived as a further potential layer of surveillance. Resilience in the banking sector also relies on intensified surveillance of banks' internal features through the application of more exacting measures, disclosures and reporting requirements.

In the case of the dictatorial regimes, wide-spread surveillance was common; in post-dictatorial regimes the lack of historical experience resulted in an increased level of vulnerability of members of these societies, and a decreased level of resilience towards new forms and technologies of surveillance.

2.2.3 Features or elements of resilience

Multi-faceted nature

The previous subsection has shown that one of the safest, but perhaps banal, things one can say about the term "resilience" is that it is multi-faceted. People perceive and define resilience in different ways. It has many different features or elements. It can be both spontaneous and ordered. Resilience can be unplanned as well as planned. People may respond spontaneously to an adverse event in a way that demonstrates resilience. Stakeholders can also plan and adopt measures aimed at increasing resilience to an adverse event. Individuals, groups, organisations, countries and critical infrastructure all share something in common, i.e., they all can be resilient. Resilience can be perceived in physical and cyber space. Resilience is a term used in various sectors, both public and private, such as the environment, the economy, health care, telecommunications, national security, disaster response, corporate recovery (or business continuity), crisis communications, aid programmes for developing countries, among others. Resilience is a response to, as well as preparation for, an adverse event that can be anticipated or unanticipated. Resilience can be a response to a short-term adverse event (a shock) as well as to a long-term stress. Resistance can be a feature of, as well as distinct from, resilience.

Communication between stakeholders

A feature or element of resilience is communications between stakeholders. We can hypothesise that resilience improves with improvements in communications networks and stakeholder interaction and understanding. However, as section 2.1.6 shows, there are risks of a "human bottleneck" when control centres are deluged with data, some of which may augur a disaster-in-waiting.

Temporality, spatiality

Resilience has a temporal as well as a spatial aspect. The term suggests that some event or stress or shock precedes a resilient response. In reality, however, the resilient

response can begin before the event or stress or shock, in the sense that government or communities or individuals may take certain steps before the adverse event in order to cope with it better when the event arrives. Planning in anticipation of the event is already a manifestation of resilience. Resilience implicitly posits the inevitability of some threats: only certain threats can be prevented; the rest must be endured, albeit with the benefit of the preparatory damage-limitation measures and infrastructures that a resilience strategy promotes, thereby increasing the likelihood of national survival or community persistence, as shown in the earlier discussion of the UK Cabinet Office.

Inability to always anticipate negative and counter-productive consequences

An important finding of the London bombings case study was that the framing of resilience measures can often benefit from lessons learned from prior events and aim to mitigate future adverse events. However, resilience measures do not always anticipate very well their sometimes negative and counter-productive consequences.

A set of core elements

As mentioned earlier, our examination of various European Commission documents shows that we can highlight several core features or elements of resilience, as follows: anticipation of vulnerabilities, threats, attacks, crises; preparedness; prevention, detection and response; mitigation; recovery and the sharing of responsibility and co-operation among stakeholders. The elements of resilience mentioned in a UK Cabinet Office document are almost the same: anticipation, assessment, prevention, preparation, response and recovery. All of these features are germane to preparation of a resilience strategy for the surveillance society and for discussing various "resilience-in-a-surveillance-society" propositions.

The European Union and its Member States have put in place measures to increase resilience and the ability to respond effectively both to the threat or occurrence of natural disasters, such as earthquakes and damage to the built environment,[249] volcanic eruptions,[250] forest fires,[251] floods,[252] landslides and man-made disasters such as marine pollution incidents or threats or actual acts of terrorism such as those experienced in Madrid in 2004 or London in 2005.[253] The EC has identified increasing resilience as a priority in three key areas: food security, climate change

[249] Alexander, David E., "The L'Aquila earthquake of 6 April 2009 and Italian Government policy on disaster response", *Journal of Natural Resources Policy Research*, Vol. 2, No. 4, 2010, pp. 325-342. See also Amaratunga, Dilanthi, and Richard Haigh (eds.), *Rebuilding for Resilience: Post-Disaster, Reconstruction of the Built Environment*, Wiley-Blackwell, 2011.

[250] Sangster, H., D.K. Chester and A. M. Duncan, "Human responses to historical eruptions of Etna (Sicily) from 1600 to present and their implications for present-day disaster planning", Conference Proceedings, EGU General Assembly 2012, held 22-27 April 2012 in Vienna, p. 8477.

[251] European Commission, *JRC Scientific and Technical Reports*, Forest fires in Europe 2008, No.9, 2009. http://forest.jrc.ec.europa.eu/media/cms_page_media/9/forest-fires-in-europe-2008.pdf

[252] Del Carmen, Llasat, and F. Siccardi, "A reflection about the social and technological aspects in flood risk management–the case of the Italian Civil Protection", *Natural Hazards Earth Systems Science*, Vol. 10, No. 1, 2010, pp. 109-119.

[253] Canel, José Maria, and Karen Sanders, "Crisis communication and terrorist attacks: framing a response to the 2004 Madrid bombings and 2005 London bombings", *The handbook of crisis communication*, Wiley, Chichester, UK, 2010, pp. 449-466.

adaptation and disaster risk reduction. Unfortunately, none of these priorities includes a discussion of how best to protect fundamental rights in a surveillance society.

Coherent set of objectives and measures

Resilience suggests a coherent set of objectives and measures aimed at achieving them in the face of typical human and natural threats to national security and community disruption. Resilience could be regarded as a form of risk management. The term "resilience" suggests strength, robustness and fortitude, features that are implicit in the discussion of resilience in the 2010 US National Security Strategy, which includes a sub-chapter the aim of which is to "strengthen security and resilience at home",[254] as well as the resilience of "citizens, communities, and economy", which is considered an important element of national security itself.

An opportunistic nature

In identifying the features and elements of resilience in today's surveillance society, it is interesting and relevant to consider resilience in the context of surveillance societies of Eastern Europe in the communist era. In that time, one could relate resilience to individual citizens, groups and institutions; they developed a capacity for resilience in regard to the political changes they experienced after World War II. From those societies, we can see that resilience has an opportunistic aspect. There are opportunities for developing stronger or better resilience that may not be possible at other times. Section 2.1.3 points out that if actors of a certain domain were able to take advantage of the opportunity for establishing their legal and institutional framework and laying down the fundamentals of a rule-of-law system, this resulted in an increased level of a specific institutional-legal form of resilience. Countries where the newly democratic governments missed the opportunity to establish these fundamentals – saying that they would leave them until popular demand arose – could never fully reach the level of early-reacting countries.

The formation of resilience of society towards surveillance in the post-dictatorial societies also deserves attention. According to Maria Los, one of the factors in the long-lasting impact of dictatorial surveillance in these societies was the "conversion of fear": after the political changes, the fear of the repressive regime was soon replaced by a fear of crime.[255] Another conclusion by Los is that societies under long authoritarian rule in the 20th century virtually skipped the period of democratic modernity and jumped directly into the surveillance culture of postmodernity. The lack of historical experience has resulted in an increased level of vulnerability of members of these societies, and a decreased level of resilience towards new forms and technologies of surveillance. As Section 2.1.3 shows, members of these societies are less experienced and more gullible vis-à-vis business and marketing offers, including industry-driven surveillance.[256]

Solidarity

---

[254] The White House, "National Security Strategy", 2010, pp.18-19.
[255] Los, Maria, "Post-communist fear of crime and the commercialization of security", *Theoretical Criminology*, Vol. 6, No. 2, 2002.
[256] Szekely, Ivan, "Hungary", in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation,* Edward Elgar Publishing Ltd., 2008.

Solidarity can be regarded as an important element of resilience too. For example, the European Union's response to civil protection (its resilience) is embedded in solidarity: "Our aim is to boost solidarity among Member States and neighbouring countries so as to achieve the optimal level of preparedness for emergencies and to ensure a rapid and effective response when disaster strikes."[257] There is an increasing trend within the EC towards providing humanitarian assistance in civil emergencies, an approach which also now often extends beyond the boundaries of the EU. This extension of EC support demonstrates a growing maturity in its recognition of the collective responsibility we have for responding to emergencies beyond the EU. Solidarity is therefore a feature of relevance to resilience in a surveillance society.

2.2.4 Is resilience always good?

Resilience is generally understood to be "good thing". No one urges *less* resilience. If anything, people are exhorted to be *more* resilient, which must mean that resilience is a good condition. Implicit in the term is the assumption that people may experience significant threats or challenges to everyday life (whether these be natural disasters, pandemics, or security threats), and that these need to be anticipated or handled in a rational manner by central government as well as others. As yet, society is yet to become resilient to surveillance and its threat to fundamental rights.

As noted in the discussion of resilience in dictatorial and post-dictatorial regimes in section 2.2 above, resilience can work to prolong the grasp on power by dictators. They may be as resilient as (or even more resilient than) the population which they govern. Hence, resilience can be a condition supporting not only good-doers, but wrong-doers such as dictators, criminals and others. The resilience of the latter categories has not served the citizenry. Additionally, surveillance has focussed mostly on "street crime" and terrorist threats rather than the depredations of our economic well-being. Furthermore, it is possible that the citizenry will suffer from "resilience fatigue" if they are being exhorted to be resilient so often and from so many different directions that they may cease to be pro-active in resilience and protecting themselves.

Different aspects of resilience in a surveillance society are especially evident in the dictatorial and post-dictatorial regimes of Eastern Europe in the years after World War II. The dictatorial elite showed resilience in supporting the old regimes and then in transforming themselves into entrepreneurs controlling important institutions and businesses in the new democracies, so that they were able to profit from the transition and/or maintain their hold on power. In the old regimes, the citizenry also showed resilience in different ways: in accommodating (grudgingly) themselves to the communist elite and/or in resisting the elite (for example, by engaging in *samizdat* publishing).

2.2.5 Elements of a resilience strategy

[257] European Commission, Humanitarian Aid & Civil Protection, European Civil Protection, Consultation on the Future Instrument Addressing Prevention of, Preparedness for and Response to Disasters, 1 December 2011.
http://ec.europa.eu/echo/civil_protection/civil/consult_new_instrument.htm

For the purpose of this report, we define a "resilience strategy" as a strategy aimed at making individuals or groups or institutions resilient in the face of whatever shock or stress. Our report is particularly concerned with resilience in a surveillance society. As with most strategies, a resilience strategy should say for whom the strategy has been prepared, the purpose of the strategy and against which stress or shock the strategy has been prepared. A wrong-doer may have a resilience strategy just as easily as someone who is a good-doer. Even the terms "wrong-doer" and "good-doer" are a matter of perspective. A government official may view Edward Snowden, who exposed the US National Security Agency's (NSA) activities, as a "wrong-doer", while to a member of the public, he may be seen as a hero,[258] one who has taken dramatic action against the surveillance society and, in this case, blown the whistle on the extent to which spy agencies spy on their own citizens. While contextual information is useful in a resilience strategy, the elements in the strategy may well apply to both the wrong-doer and the good-doer. For example, both "doers" may generate significant media attention as a way of promoting resilience. Communication and networking are likely to be important elements in most resilience strategies, but perhaps not in all. For example, the strategy of some wrong-doers involves avoiding drawing attention to themselves, i.e., shunning communication.

The EU has arguably "operationalised" resilience to some extent through the so-called the Community Mechanism for Community Protection which provides evidence of governments engaging communities in regard to civil protection and resilience.[259] Since creation of the Community Mechanism in 2001, it has been invoked or come into play more than 150 times. Training is part of civil protection and resilience. While this operationalisation of resilience in the civil protection domain is important and has a bearing on the surveillance society, others in addition to the civil protection stakeholders need to be involved in developing a resilience strategy for the surveillance society.

The brief review of EC documents earlier concluded by identifying various elements that could be part of a resilience strategy. Adding slightly to this, in order to make systems, individuals, groups and society resilient, measures that could contribute to a more robust resilience strategy include the following:

1. Policy dialogue
2. Good risk management and sound risk methodologies and vulnerability assessment
3. Standardisation
4. Increased transparency
5. Regional and/or international approach to resilience rather than only a national approach
6. Multi-stakeholder approach
7. Stakeholder collaboration and co-ordination
8. Flexibility
9. Innovation
10. Learning lessons from past or concurrent experience elsewhere.

---

[258] Walt, Stephen, "Snowden deserves an immediate presidential pardon", *The Financial Times*, 8 July 2013.
http://www.ft.com/cms/s/0/0ccf2d14-e7c1-11e2-babb-00144feabdc0.html#axzz2YiI70RAU

[259] European Commission, "The Community Mechanism for Civil Protection". http://ec.europa.eu/echo/policies/disaster_response/mechanism_en.htm

The term "resilience" can incorporate preventive strategies, emergency planning, contingency strategies and recovery strategies. A governmental resilience strategy may include dissemination and co-ordination among different agencies and at different levels of government. Resilience strategy may include planned, co-ordinated efforts across organisations at different levels of a national system, and among participants with defined roles and responsibilities.

While in the 2010 National Security Strategy, the achievement of a resilient nation is based on the recognition and nurturing of a resilient society (and economy), in the 2007 Homeland Security strategy, it is the protection of critical infrastructure and key assets that facilitates the building of "a more resilient Nation".[260] Even if resilience refers to "material" conditions, the same document also introduces the notion of "operational resilience", which refers to the ability to ensure organisational continuity in case of disaster.[261] While it is not clear what would be the practical elements of this kind of resilience, apart from the set-up of "continuity programs",[262] we can deduce that solutions that go beyond the material survival of structures and networks should be considered.

The UN International Strategy for Disaster Reduction (UNISDR) places emphasis on data collection and analysis of evidence, as well as international co-operation, as part of a strategy of prevention, emergency preparedness, risk reduction and resilience-building. As stressed earlier, a good resilience strategy should involve a wider group of actors, sharing both forces and responsibilities for the (continuous) preparation against adverse events, punctual mobilisation in case of disruption and collectively responding to the challenges of surveillance. This can be applied to a resilience strategy for surveillance as well.

Resilience strategy should include provision for protecting human rights that may be compromised in responses to crime, drugs and terrorism, as the contribution on the UN and resilience showed, indicating that a resilience strategy should identify the threat, what is threatened, and how the threat can be countered through preventive or remedial measures. Resilience strategy should include provision for both preventative and preparedness measures, which are not the same thing.

Some key features or elements of a resilience strategy against surveillance can be derived from our analysis of resilience in different domains:

- the ability to identify and mitigate specific challenges of surveillance
- an examination of the different social aspects as well as how surveillance takes place in different sectors of our economy
- the acknowledgement of the complexity of systems and the high reliance of societal activities on them;
- the acknowledgment of the impossibility to ensure maximal security, and the need to accept risk(s), and to eschew the trade-off paradigm where security is balanced against privacy or other fundamental rights;
- the need to foresee and prepare against aggressive instances of surveillance;

[260] "By protecting CI/KR, we further protect the American people and build a safer, more secure, and more resilient Nation"; ibid., p. 25.
[261] Ibid., p. 29.
[262] Ibid.

- the need to rally different and new actors, sharing responsibilities, knowledge and resources with them;
- the institutionalisation of the latent strengths, in order to be able to calculate them in foresight exercises, and to nurture and train stakeholders;
- communication and the structure of communications.

Several policy tools can be employed in the development of a resilience strategy. A crucial policy tool is the formulation of comprehensive strategic plans, with specific goals and objectives. Public-private partnerships might help in resilience strategies. The engagement of societal actors tends to be a specific way to institutionalise resilience and their relative latent strengths. This strategy could be applied by both the surveillants and civil society organisations or privacy advocacy groups. A risk-management approach will help identify threats, vulnerabilities and the best solutions to reduce the consequences of disruption. Redundant systems and technological innovation can also form part of a resilience strategy (which could especially be applicable to the surveillants).

2.2.6 Key resilience stakeholders

The various EC documents analysed before in this deliverable show that a resilience strategy may be addressed to any of the following cases: *failures, attacks, risks, disruptions, disasters, hazards, threats, stresses, shocks, crisis, uncertainty* and *change.* These documentary initiatives confirm the European Commission as a key stakeholder in developing a Europe-wide resilience strategy. While the EC assumes this role, it also extends its resilience network to academic researchers, civil society organisations and other stakeholders. The European Commission's 2012 Security Work Programme particularly encouraged research proposers to "to develop solutions strengthening societal resilience and active participation of citizens as security enhancing resources".[263] Resilience also featured in the Commission's Socio-Economic Sciences and the Humanities (SSH) Work Programme of 2012,[264] which called for the establishment of new mechanisms to "reinforce economic policy coordination needed to ensure the EU is more resilient, and able to effectively prevent major economic instabilities in the future".[265] The SSH Work Programme also focused on citizens' resilience in times of crises. It suggests that "understanding how citizens claim and enact their rights and how they develop resilience in difficult times is crucial for both the EU and its Member States".[266]

In US security strategy documents, the role of private companies is not assessed in terms of their potential negative effects on society and individuals, e.g., the possible negative consequences of reinforced private surveillance in the workplace of critical infrastructures. On the contrary, national strategies seek to engage stakeholders from the private sector, especially those operating critical infrastructures.

---

[263] ftp://ftp.cordis.europa.eu/pub/fp7/docs/wp/cooperation/security/k-wp-201201_en.pdf
[264] FP7-SSH-2012-2. European Commission C (2011)5068 of 19 July 2011.
[265] OJ C213 of 20 July 2011.
http://ec.europa.eu/research/participants/portal/page/call_FP7?callIdentifier=FP7-SSH-2012-2&specificProgram=COOPERATION#wlp_call_FP7
[266]http://ec.europa.eu/research/participants/portal/page/call_FP7?callIdentifier=FP7-SSH-2011-2&specificProgram=COOPERATION#wlp_call_FP7

UN Secretary-General Ban Ki-moon address on "Resilience and solidarity: our best response to crisis", to the World Health Assembly in May 2009 portrays "resilience" as primarily a matter of bureaucratic preparedness. There does not seem to be such a need for citizen engagement. However, the WHO produced a popular, illustrated manual on dealing with a mental health crisis in which citizen engagement is manifest.

While people should be resilient in face of any disruptive event, their preparedness should not let the private sector or the government off the hook; the private sector and governments should not shirk their responsibilities toward individuals (citizens and consumers), groups and other institutions. As the preceding paragraphs indicate, resilience is becoming a political issue of some consequence. Accountability should be spelled out explicitly in any overall strategy, which should include provision for awareness-raising and informing citizens about the importance of resilience.

National governments also play a key role in resilience. For example, the UK government takes an active role in building resilience, and does not just slough off responsibility onto citizens. It provides guidance on emergency planning, resilience and preparedness; exercises and training; national recovery guidance on humanitarian issues, economic issues, infrastructural issues, plus telecoms resilience.[267] The Government's resilience to major events has been demonstrated at a national level through the establishment of a civil emergencies committee, commonly known as the COBRA Committee. The Cabinet Office provides advice to individuals and networks in the form of a guide on Integrated Emergency Management (IEM)[268] which covers "anticipation, assessment, prevention, preparation, response and recovery. The Cabinet Office also stimulates collaboration with the voluntary sector too. It has established the Voluntary Sector Civil Protection Forum, which is a grouping of voluntary organisations that have a civil protection role, and provides advice.

The review of domains shows that there are potentially quite a few different stakeholders who could be involved in the development of a resilience strategy in the surveillance society. In the domains examined, there is little direct mention of the surveillance society, surveillance undertaken by governments and corporations, or how resilience might play a role in the surveillance society. Nevertheless, the review of domains has helped to clarify how the term "resilience" is used in different contexts, how it is defined (or not) in different contexts, some of it's the elements or features that could be adopted in the formulation of a resilience strategy in a surveillance society. In some domains, surveillance can be an element in a resilience strategy, for example, where regulatory authorities "surveil" the banking industry or, for that matter, surveil the surveillance industry (those who manufacture surveillance products or operate surveillance services) to see how privacy and other fundamental rights are being compromised.

---

[267] UK Government, Cabinet Office, Inside Government, Public safety and emergencies, What we're doing, https://www.gov.uk/government/topics/public-safety-and-emergencies. See also UK Government, National recovery guidance, generic issues: social media, London, 4 Oct 2012. https://www.gov.uk/government/publications/national-recovery-guidance-generic-issues-social-media.

[268] UK Government, Cabinet Office, Resilience in society: infrastructure, communities and businesses. https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses#corporate-resilience-sme-resilience-strategy.

3 THE VULNERABILITY AND RESILIENCE OF DEMOCRATIC SOCIETY

This section focuses on how the open nature of democratic societies can make them more vulnerable to attacks on infrastructures or people and how, at the same time, it can make them more resilient to those attacks in terms of social, economic and institutional responses. It has been said that democratic countries that subscribe to the full meaning of an open society will be more vulnerable than most, because democracy necessarily allows and even encourages the expression of difference and a culture that welcomes opposition of views and beliefs.[269] Studies have shown the importance of social capital in resilience. For example, recovery from natural and other disasters does not depend on the overall amount of aid received nor on the amount of damage done by the disaster; instead, social capital – the bonds which tie citizens together – functions as the main engine of long term recovery.

This section involves a comparative analysis of past and current experiences in Europe and elsewhere. It examines and analyses the societal, economic and institutional responses to a number of adverse events (one-off and stressing events). It also looks at the open nature of society and its relationship with resilience and vulnerability.

3.1 SOCIETAL, ECONOMIC AND INSTITUTIONAL RESPONSES TO SELECT ADVERSE EVENTS

In the following section are a diverse set of adverse events which have been grouped in two sub-sections. In the first group are one-off events, with a shock or shocking impact – or a series of the same kind of events that share the following characteristics: sudden, devastating, hazardous, violent or catastrophic. These are events for which citizens and society can only be prepared to a certain degree. Many of them are terrorist attacks with a legacy and a long aftermath, following which new prevention measures are developed to address similar future threats. These type of events generally do not happen twice at the same location, although the attacks might be similar. Context and origins may vary, but structurally they are the same. In this group are the following adverse events:

- 11 Sept 2001 attacks
- The Madrid train bombings, 2004
- The London bombings, 2005
- The Mumbai terrorist attack
- Boston bombing 2013
- School shootings in Germany
- Christchurch earthquake

The last adverse event differs from the others to the extent that it is a "natural" disaster in contradistinction to the other listed events. However, this event too is sudden, devastating, hazardous, violent and catastrophic. There are some possibilities of being better prepared to deal with these events. However, some actions such as building houses on river banks will heighten the likelihood of destruction caused

[269] Burnell, Peter, and Peter Calvert, "The Resilience of Democracy: An Introduction", *Democratization*, Vol. 6, No. 1, 1999, pp. 1-32 [p. 17].

during such adverse events. The way culture (society) develops and shapes its environment shapes the effects of such events.

The case studies also include stressing events – events that continue for some period of time. These events are not really "events" per se, but something different. They share the following features or characteristics: they involve the collection of data in vast amounts, they are objects of public debate, they represent infringements of fundamental rights in some form, they are long-lasting, and involve various social, economic and political actors. Often they have no real starting point, but do have a legacy. When they become manifest, they may seem to resemble an event, but are more in the nature of a revelation of things past and present. The effects cannot be measured as clearly as with a terrorist attack. In this group are the following:

- 2008 Global financial crisis
- Google Street View collection of payload data
- UK National DNA Database and the case of S v. Marper
- NSA revelations

The financial crisis is somewhat different. It falls somewhere within the first and second groups –it may be a bit like a "bomb" if a bank goes bankrupt and pulls people down with it into debt with catastrophic effects on their lives. However, these effects are not clearly visible and more abstract then the impact of a real bomb. In the instance of the NSA scandal, the NSA and its political leaders took certain actions and miscalculated, which is clearly in the nature of a risk. Here the relationship between risks and resilience become important: risk management may be an element of resilience as opposed to security measures against assumed threats, which may have an adverse effect. The NSA does not appear to be engaged in risk management, but is trying to work against unknown threats with an adverse measure of unrestrained surveillance.

Each of these events will present, as relevant:

1. The nature of the adverse event (stress, shock, impact)
2. Institutional response (policy-makers, regulators, enforcement)
3. Societal response (civil society, media, academia, community, individuals)
4. Economic response (where relevant)
5. Critical conclusions from an IRISS perspective (what factors contributed to or increased vulnerability and/or what lessons can we learn re best practices that foster resilience?)

3.2 ONE-OFF EVENTS, WITH A SHOCK OR SHOCKING IMPACT

3.2.1 11 September 2001 attacks ("9/11")

Dr Rocco Bellanova, Peace Research Institute Oslo

> At 8:46 on the morning of September 11, 2001, the United States became a nation transformed.[270]

[270] 9/11 Commission, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United*

> [Derrida:] We do not in fact know what we are saying or naming in this way: September 11, *le 11 septembre*, September 11.[271]

Introduction: the relevance of the 11 September 2001 attacks for IRISS

The attacks perpetrated on the United States on 11 September 2001, have become a sort of a landmark in recent history. They have been, and still, are at the centre of institutional, policy, media, and scientific debates. To some extent, this event can be considered the *event* par excellence, particularly from the perspective of surveillance and resilience.

However, discussing the attacks of 11 September 2001, their role and consequences, their understanding, the reactions to them, remains an extremely challenging task. On one side, there is a vast amount of scientific and policy literature already published on the subject extensively covering and analysing the attacks. The very possibility of a systematic review and analysis of this vast literature is out of the scope of this deliverable, and would require a massive effort of research. For example, an online search for 'September 11' on Google Scholar provides more than 1,300,000 results.[272] On the other side, even a brief analysis of some institutional and scientific publications highlights how many different things are often conflated into the analysis of September 11, with the attacks themselves partially moving to the background of the reading, and with most of the attention focusing on the consequences attributed to them.

From the perspective of the IRISS project, and in particular the framework of this deliverable, it is worth considering what the framing of the attacks of 11 September 2001 into the event of *September 11* or *9/11* can teach us. It is important to start questioning the very possibility of providing a univocal description of the nature of the 'adverse event'. This does not mean questioning the very materiality of the attacks, the historical facts and consequences on human lives. It rather implies appreciating how the material, the symbolic and the epistemological, tend to become strictly entwined into the analyses. Four very different documents provide valuable insight on these entanglements: the executive summary of the 9/11 Commission Report; a philosophical reading of September 11 provided by Jacques Derrida; a critical review of surveillance post-9/11 proposed by David Lyon; and a 2002 statement for the record of the then Director of the US National Security Agency (NSA) addressed to members of the US Congress and Senate.

States. Executive Summary, US Government Printing Office, Washington, DC, 2004, p. 1 [Hereinafter: 9/11 Commission Executive Summary]

[271] Borradori, Giovanna, Jürgen Habermas, and Jacques Derrida, *Philosophy in a Time of Terror. Dialogues with Jürgen Habermas and Jacques Derrida*, The University of Chicago Press, Chicago, 2003, p. 86.

[272] The search covers the publications indexed by Google Scholar, and is limited to publications in English released between 2001 and 2014. The search was carried on 18 June 2014. A similar search for the term '9/11' provided around 1 million results, but this figure is quite problematic, as Google Scholar seems to include very spurious hits (e.g. the page interval 9-11).

The 9/11 Commission Report

The 9/11 Commission Report provides a brief and powerful description of the attacks in the Executive Summary:

> An airliner travelling at hundreds of miles per hour and carrying some 10,000 gallons of jet fuel plowed into the North Tower of the World Trade Center in Lower Manhattan. At 9:03, a second airliner hit the South Tower. Fire and smoke billowed upward. Steel, glass, ash, and bodies fell below. The Twin Towers, where up to 50,000 people worked each day, both collapsed less than 90 minutes later.
>
> At 9:37 that same morning, a third airliner slammed into the western face of the Pentagon. At 10:03, a fourth airliner crashed in a field in southern Pennsylvania. It had been aimed at the United States Capitol or the White House, and was forced down by heroic passengers armed with the knowledge that America was under attack.[273]

The four terrorist attacks were planned and carried out by al-Qaida operatives, and were based on the coordinated hijacking of commercial flights and their use as weapons. The total number of victims was particularly high: according to the 9/11 Commission Report, "more than 2,600 people died at the World Trade Center; 125 died at the Pentagon; 256 died on the four planes".[274] Given their scale and their location, the attacks that occurred in New York and at the Pentagon were widely and immediately covered by the media, with the impact of the second airplane on the South Tower televised in real time.

The 9/11 Commission Report, and the constitution of the National Commission on Terrorist Attacks upon the United States, generally known as the 9/11 Commission,[275] are part of the institutional reactions to the attacks. Set up by legislation in late November 2002, the 9/11 Commission aimed to "provide a "full and complete accounting" of the attacks of September 11, 2001 and recommendations as to how to prevent such attacks in the future".[276] The 9/11 Commission was a bi-partisan and independent commission, composed of 10 members of the US Congress (5 Republicans and 5 Democrats), supported by dedicated staff and carrying on studies, interviews and hearings. The final report released on July 2004 is a comprehensive overview of the results achieved and the material used.[277] The Executive Summary provides a very telling narrative of the attacks and the main recommendations.[278]

The description of the attacks, quoted above, is linked, in the rest of the document, to an assessment of the way in which the attacks were prepared, and of the inability of the authorities to prevent it. Embedded in the report is the message that "[t]he 9/11 attacks were a shock, but they should not have come as a surprise".[279] This is one of the main conclusions of the 9/11 Commission, and a lens to better understand what happened. Despite the peculiar magnitude of the attacks, the 9/11 Commission traces

---

[273] 9/11 Commission Executive Summary, op. cit., 2004, p. 1.
[274] Ibid., pp. 1-2.
[275] The National Commission on Terrorist Attacks Upon the United States. http://govinfo.library.unt.edu/911/about/index.htm
[276] The National Commission on Terrorist Attacks Upon the United States. http://govinfo.library.unt.edu/911/about/faq.htm#q2.
[277] 9/11 Commission, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, US Government Printing Office, Washington, DC, 2004.
[278] 9/11 Commission Executive Summary, op. cit., 2004, p. 1.
[279] Ibid., p. 2.

continuities: al-Qaida was already a threatening organization, and several attacks had already been carried on, at least since 1998. Further, "the most important failure was one of imagination", imagination of the authorities and leaders in failing to understand "the gravity of the threat".[280] The inability to properly assess the 'quality' of the novelty, to appreciate if the threatening organisation was a "new and especially venomous version of the ordinary terrorist threat" or a "radical novelty", was a key shortcoming.[281] So, at the same time, the attacks were new and in continuity with the recent past, at the same time something that could have been diverted, and that necessitates a re-think of the ways in which counter-terrorism is carried out.

To some extent, the attacks become an event as they are understood beyond their material facts. Their very possibility of occurring is connected to a wider picture and many other elements, including the failure of previous policies, strategies and analysis. It is from this perspective that the recommendations make sense, and long-term responses to the attacks can be planned. The nature of the attacks is such that they could recur, thus they are potentially not just a one-off.

In the aftermath of the attacks: a philosophical reading of an 'event'

While it is always difficult to disentangle the material and the symbolic natures of terrorist attacks, the attacks of 11 September 2001 were immediately framed as a *major event* by Western media, policy makers and several commentators. The common reference to the attacks through the use of the date – September 11 or 9/11, often without mention of the year – seemingly confirm, and reiterate, this framing; and it is still very common even in policy and academic literature. However, as Derrida noted, this reference is only apparently self-evident or self-explaining: "name, repeat, rename "September 11," "le 11 septembre," even when you do not yet know what you are saying and are not yet thinking what you refer to in this way".[282] Interviewed in the aftermath of the attacks, Derrida explained the difficulty of understanding what happened (without disputing what happened):

> The brevity of the appellation (September 11, 9/11) stems not only from an economic or rhetorical necessity. The telegram of this metonymy – a name, a number – points out the unqualifiable by recognizing what we do not recognize or even cognize, that we do not yet know how to qualify, that we do not know what we are talking about.[283]

The challenge of understanding what happens or happened, is an integral part of the event. According to Derrida, 9/11 is an event in so far as we fully realize the defying nature of the same:

> [t]he event is what comes and, in coming, comes to surprise me, to surprise and to suspend comprehension: the event is first of all *that which* I do not first of all comprehend. Better, the event is first of all *that* I do not comprehend. It consists in *that*, *that* I do not comprehend: *that which* I do not comprehend and first of all *that* I do not comprehend, the fact that I do not comprehend: my incomprehension.[284]

The attacks oblige one to embrace the lack of comprehension; they oblige one to think carefully their implications. They are not self-evident; questioning how they are

[280] 9/11 Commission Executive Summary, op. cit., 2004, p. 9.
[281] Ibid.
[282] Derrida, op. cit., 2003, p. 88.
[283] Derrida, op. cit., 2003, p. 86.
[284] Derrida, op. cit., 2003, p. 90 (italics in original).

understood permits one to understand better the consequences linked to them.

From this perspective, Derrida proposed understanding the emerging logic of response to this lack of comprehension as an "*autoimmunitary process*": a "strange behavior where a living being, in quasi-*suicidal* fashion, "itself" works to destroy its own protection, to immunize itself *against* its "own" immunity".[285] Conversely, the event itself includes the reactions to the same, and especially the way in which the future is to be understood:

> "it is the future that determines the unappropriability of the event, not the present or the past. Or at least, if it is the present or the past, it is only insofar as it bears on its body the terrible sign of what might or perhaps will take place, which will be *worse than anything that has ever taken place*".[286]

What we can learn from Derrida's analysis, is that an event can be understood beyond its specific happening. For example, 9/11 is not a self-evident thing but the irruption of a series of open questions. This seems to be confirmed by the 9/11 Commission Report: there, 9/11 should and can only be understood through the responses to a series of questions that emerged from the very experiences; the event has to be reconstructed despite the attacks themselves being known to everybody. The traumatism and the potential remedies have to be considered not only in relation to the historical facts, to what happened, but by comprehending the event and the set of possibilities that it may recur. To some extent, an event is neither univocal nor fixed in time, but always to be framed in continuity with both the past and the future.

9/11 as epistemological tool: reading the surveillance responses to 9/11

According to David Lyon, 9/11 should be read in connection to the responses to the attacks:

> The September 11, 2001 terrorist attacks on New York and Washington prompted a series of responses, from military retaliation on the country harbouring Osama bin Laden to extensive anti-terrorist legislation aimed at domestic protection.[287]

From Lyon's point of view, 9/11 cannot be understood without taking into account the responses. His focus is on surveillance measures. More interestingly, and in implicit resonance with the other two documents analysed above, Lyon proposes conceiving 9/11 as a prism or a lens to better understand continuities and novelties in the surveillance landscape.[288] From his viewpoint, specific trends emerge, and in particular the widening and fostering of existence surveillance practices, and a further reliance on technologies. The main novelty seems to be the emphasis on the use of profiling and social sorting systems, purportedly aiming at identifying threats and threatening individuals in advance.[289]

---

[285] Derrida, op. cit., 2003, p. 94 (italics in original). On the relation between immunisation and the making of political community, see Esposito, Roberto, *Terms of the Political. Community, Immunity, Biopolitics,* Fordham University Press, New York, 2013.
[286] Derrida, op. cit., 2003, p. 97 (italics in original).
[287] Lyon, David, "Surveillance after September 11, 2001", in Kirstie S. Ball and Frank Webster (eds.), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, Pluto Press, London, 2003, pp. 16-25, [p. 16].
[288] Ibid., p. 17.
[289] See also Gandy, Oscar H., "Data Mining and Surveillance in the Post-9/11 Environment", in Kirstie S. Ball and Frank Webster (eds.), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, Pluto Press, London, 2003, pp. 26-41.

This growing attention to profiling is also confirmed in the recommendations of the 9/11 Commission, especially in relation to the profiling of flight passengers.[290] However, the emphasis on profiling permits Lyon to note another important feature of post 9/11 surveillance:

> Though very powerful searchable databases are in use, and those in intelligence and policing services are being updated after September 11, the all-important categories with which they are coded […] are produced by much more mundane processes. Database marketers in the US use crude behavioural categories to describe neighbourhoods […] and CCTV operators in the UK target disproportionately the 'young, black, male' group. The high-tech glitz seems to eclipse by its dazzle those social factors that are constitutionally imbricated with the technical.[291]

The interesting point is that some of the profiling or profiling-like systems were already in use; however, these systems should be understood in a political economy made up of private companies developing the technologies and the relevant categories. Consequently, technological fixes carry their own economic, political and social legacies, and they not only respond to the event, but are (at best) adjusted to respond to the event, and the possible recurrence of the event.

Though Lyon's focus is explicitly on the responses to the event, rather than the attacks themselves, the analysis of the responses highlights a growing autonomy of the responses to the supposedly triggering event. The term 9/11 refers less to what happened on a specific day, and increasingly to a set of actions, policy choices, and even a sociological debate about the role of the event (continuity, discontinuity, novelty, legacy etc.).

An example of institutional discourse: the NSA reaction to 9/11

Around a year after the attacks, on 17 October 2002, the then Director of the US National Security Agency and Chief of the Central Security Service publicly testified before the Joint Inquiry of the Select Committees on Intelligence of the Senate and the House.[292] As in the 9/11 Commission Report, this document is the product of one of the institutional responses to the attacks, one of the inquiries carried on by the US Congress.

The document is particularly interesting because "it is one of the few times in the history of [NSA] that the Director has testified in open session about operational matters".[293] NSA was, and increasingly is, a key player in counter-terrorism and surveillance in general, but rather secretive (e.g. its budget is not made public). For the purpose of this section, the Statement for the Record of the then NSA Director permits us a closer look at the formulation of an institutional discourse that further articulates the different elements of 9/11.

The speech is divided into three main parts, each responding to a key question: "what did NSA know prior September 11", "what has NSA learned in retrospect", and "what

---

[290] 9/11 Commission Executive Summary, op. cit., 2004, p. 19.
[291] Lyon, op. cit., 2003, p. 23.
[292] Hayden, Michael V., *Statement for the Record by Lieutenant General Michael V. Hayden, Usaf, Director, National Security Agency/Chief, Central Security Service before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence*, 17 October 2002, National Security Agency/Central Security Service, Washington, DC, 2002.
[293] Hayden, op. cit., 2002, § 36.

has NSA done in response".[294] The organisation of the statement itself frames the attacks of 11 September 2001 in a rather linear temporality, from which the very attacks are largely bracketed off. Still, there is a constituting tension between the role of the attacks themselves and how they should be understood.

On the one side, 11 September 2001 is mentioned mainly at the very beginning of the speech, to underline that the "[NSA] workforce takes the events of September 11, 2001 very personally".[295] Then, again, towards the end of the speech, the day of the attacks and the "events" themselves are portrayed as the historical and rare occasion to reflect, "readdress" one of the "serious issues" and "to find the right balance between protecting our security and protecting our liberty".[296]

On the other side, the attacks provide further information and guidance on the dynamics of the NSA as an institution. For example, the then NSA Director resists the criticism about "some culturally based "failure to share"".[297] Before the actual attacks, it did not make sense to share specific bits of information available because they were still "unexceptional" in the actual context.[298] Furthermore, and somehow paradoxically, September 11 is presented as confirming a need to complete an already occurring "transformation".

In other words, the September 11 attacks were a shock, even for the NSA workforce, but they are presented by the then Director as a means of confirming policy choices that the NSA had already taken before the attacks themselves. In particular, rather than demonstrating failure, the event confirmed the interpretation of the past provided by the NSA. For example, the discourse argues that the ongoing information revolution needs to be taken into account in the funding and staffing of the NSA, to ensure the relevance of the agency and its capacity to provide actionable intelligence, given the growing use of information technologies.

As noted in the analysis of the other documents, the past and the future contribute to the interpretation of this event. The legacy of past experiences, future expectations and visions, play a key role in the definition and description of the event. These different legacies and future aspirations contribute to the framing of the same attacks into different types, necessitating different kinds of responses. Among the specific responses envisioned by the NSA, this discourse promotes the advantage of a public-private partnership and of an outsourcing strategy, as a form of ensuring efficiency.[299] Again, the strategy is not a mere reaction to the event; September 11 rather seems to confirm the appropriateness of the strategy itself. The reference to the growing role of the private sector resonates with Lyon's analysis, even if no critical remarks on the specific legacy of this kind of political economy were advanced.

Finally, it is relevant to return to the framing of September 11 as a renewed occasion to "find the right balance between protecting our security and protecting our liberty".[300] The then Director of the NSA notes that he had been questioned by the Congress about the NSA's ability in "safeguarding the privacy rights of those

[294] Hayden, op. cit., 2002.
[295] Hayden, op. cit., § 2.
[296] Hayden, op. cit., § 41.
[297] Hayden, op. cit., § 9.
[298] Hayden, op. cit., § 10.
[299] Hayden, op. cit., § 27.
[300] Hayden, op. cit., § 41.

protected by the U.S. constitution and U.S. law".[301] To some extent, the NSA is presented as a rather stable agency, with a clear mission, whose achievement also depends on the way Congress sets the privacy-security balance. From this perspective, the very idea of the need for a balance, and of a zero-sum game relation between security and privacy is 'naturalized': the NSA reading of 11 September 2001 as an historical landmark contributes to this.

Critical conclusions from an IRISS perspective

While the other events analysed in this report are widely known, the attacks of 11 September 2001 are particularly significant in discussing resilience and surveillance. 11 September 2001 (or alternately 9/11 or September 11) is generally perceived as a self-explaining and self-evident event. For this reason, the goal of this section was not to present an overview of all the already documented institutional, societal and economic responses, but rather to problematize the concept of event. From an IRISS perspective, the analysis of the four readings of the '9/11 event' offers the following insights:

- It is extremely challenging to disentangle the material, social and epistemological aspects of an event. Both actors and analysts can only conceive of an event as a mix of these different elements.
- An event is not confined to specific and given facts and dates. This does not imply denying the occurrence of historical facts. It rather invites one to be aware that these facts are clustered with many others, and are framed in different ways. 'One-off events' do not happen in vacuum, and they are rarely perceived as something unique. Despite the shock, the event connects heterogeneous elements, and relates to both the past and the future.
- The event is particularly important in relation to the possibilities it may open up, and in particular to the possibility that it may happen again. It generates a sort of anxiety for the future: the recent past itself is re-assessed against different visions of incumbent futures.
- The event also includes the responses to it: it can be understood with, and through the responses formulated to it. The event and its responses function as a key, or a prism, to understand not only what happened, but also what is happening and what may happen.
- The use of a shared label (e.g. 9/11 or September 11) by different people and actors does not imply that they all share the same understanding or description of the event. It rather signals that there is a constant uncertainty about what an event stands for, and that asserting a discourse about the event is a way to stabilize it.
- Discussing the impact and importance of an 'event' in terms of continuity or radical change is not particularly promising. It is more promising to decrypt what different actors put in continuity or discontinuity, in their framing of the event.
- Finally, attention to the auto-immunitarian reactions to an event may prove particularly fruitful when focusing on surveillance and resilience, and the blurring of the two.

[301] Hayden 2002, § 37.

3.2.2 The Madrid train bombings, 2004 ("11M")

Professor Charles Raab and Dr Richard Jones, University of Edinburgh

Nature of the adverse event

Three days before the Spanish general election, on the morning of 11 March 2004, 10 backpack bombs exploded on four rush-hour commuter trains in Madrid. 191 people were killed and more than 1,800 others were injured. At a train station through which the four trains had passed, the police later found a van containing bomb detonators as well as a tape-recording of verses from the Koran. The next day, the police deactivated a bomb with a mobile phone as a detonator, which had been in a backpack they found on one of the trains. Two days following the bombings, the police arrested a Moroccan-born man who had sold the pre-paid cards that were used in the detonators. A video found near a Madrid mosque showed that al-Qaeda in Europe claimed responsibility as revenge for the presence of Spanish troops in Iraq and Afghanistan, although the involvement of al-Qaeda has been disputed.[302] On 26 March, detonators, dynamite traces and fingerprints were found inside a country cottage where police suspected the bombs had been manufactured.

As the police converged on a flat outside Madrid on 3 April, seven suspects blew themselves up; a Special Forces soldier was also killed in the blast. The police described the dead suspects as ringleaders; one suspect escaped but was later apprehended in Serbia. Although the Basque separatist ETA organisation was first suspected of involvement, attention later switched to the Islamic extremist Moroccan Islamic Combatant Group (GICM). Two years later, in 2006, 29 people were indicted for the bombings, of whom 15 were Moroccans, nine Spaniards, two Syrians, one Egyptian, one Algerian and one Lebanese. Charges were eventually dropped against one of them when the case was tried in 2007. One person had already been convicted in 2004 (a 16-year old boy who had stolen and carried the explosives used in the bombings), while many others remained in detention on provisional charges or were released.[303]

The Madrid bombings were the worst event of their kind in Europe since the Lockerbie bombing in 1988, and far worse in their death and injury toll than the ETA bombing of a supermarket in Barcelona in 1987. Madrid and other Spanish locations had experienced terrorist activities and atrocities over many years since the 1960s, the frequency and scale of which peaked in the late 1970s and 1980s, but ETA perpetrating such activities had been on the wane in more recent years although it still carried out terrorist activities sporadically in the 1990s.

Institutional response

Given the proximity of the bombings in the run-up to the general election, the main political parties in Spain quickly accused each other of concealing or distorting

[302] Corera, Gordon, "The legacy of the Madrid bombings", *BBC News*, 15 February 2007. http://news.bbc.co.uk/1/hi/world/europe/6357599.stm

[303] The Guardian, "The 2004 Madrid bombings", *The Guardian*, 31 October 2007; Globalsecurity.org, "Madrid Train Bombing", 13 July, 2011. http://www.globalsecurity.org/security/ops/madrid.htm

evidence, and the governing party blamed ETA. In the election, the Spanish Socialist Workers' Party under José Luis Rodríguez Zapatero replaced the conservative Partido Popular government of José María Aznar. A few weeks after the election, the new government withdrew Spanish troops from Iraq.

An increase in surveillance over several years was one response. Galdon Clavell et al. found that "there is no evidence of an immediate increase in surveillance in the country capital following the attacks".[304] However, another source – perhaps reporting a later development – states that, in the aftermath of "11M", there were introduced "additional surveillance measures including an increase in the number of security forces in locations where there are large numbers of people, notably airports, train stations and the Madrid Metro system. Local police now patrol the Metro lines and the army is helping to monitor the railroad infrastructure throughout Spain. Sensitization campaigns have also been carried out for the population so that the people can report any abnormalities they have witnessed."[305] There has also been an increase in video surveillance in rail transport: it is reported that "[s]ince the attacks, stations have been retrofitted with anti-intrusion and detection systems, and additional surveillance cameras and private security officers are now employed to monitor patron and employee areas".[306]

A 2013 article, reporting on the ability of the police and security services to act and react in 2004, points to the underdevelopment of available technology at the time of the bombings.[307] Richard Huelin, a retired army colonel, said that phone-tapping was the main mode of surveillance, as the use of CCTV was embryonic and of limited use in terms of storage and quality, so that it was difficult to analyse images for intelligence purposes. In Atocha, the Madrid rail station that was affected by the events, camera images were grainy and distant, revealing no clues about the bombers; there were no cameras at the suburban stations where the suspects boarded the trains. Therefore, the police had to fall back on examining chemical explosives to identify their source, and on tracing the origin of the detonators' SIM cards.
In contrast, in 2013, "[p]assengers arriving at the Atocha station are filmed from the second they step off the train until they exit the station by state-of-the-art, high-resolution cameras".[308] A retired military intelligence source, Javier Vidal, says that Spain is now a society under watch: "You leave your house for work and you're filmed by multiple cameras… [a]t the pharmacy, the tobacco shop, at banks."[309] The article observes that security experts believe that "with today's technology, authorities

[304] Galdon Clavell, Gemma, Lohitzune Zuluoga Lojo and Armando Romero, "CCTV in Spain: An Empirical Account of the Deployment of Video-Surveillance in a Southern-European Country", in C. William R. Webster, Eric Töpfer, Francisco Klauser and Charles D. Raab (eds.), *Video Surveillance: Practices and Policies in Europe*, IOS Press, Amsterdam, 2012, pp. 133-144 [p. 135].
[305]TravelVideo.TV, "Spain tourism in excellent health despite Madrid bombing", *TravelVideo.TV*, 3 May 2004, quoting Miguel Angel Villanueva, Madrid's head of finance and tourism development. http://www.exceltur.org/excel01/contenido/portal/files/MAY_04_093.pdf
[306] Transit Cooperative Research Program, *Video Surveillance Uses by Rail Transit Agencies – A Synthesis of Transit Practice*, TCRP 90, Transportation Research Board, Washington, DC, 2011, p. 18, (citing Loukaitou-Sideris, A., B.D. Taylor, and C.N.Y. Fink, "Rail Transit Security in an International Context: Lessons from Four Cities", *Urban Affairs Review*, Vol. 41, No. 6, 2006, pp. 727–748 [p. 740]). http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_syn_90.pdf
[307] Hadden, Gerry, "Spain Invests in Technology to Fight Terrorism", *The World*, 29 May 2013. http://www.theworld.org/2013/05/spain-invests-in-technology-to-fight-terrorism/
[308] Ibid.
[309] Hadden, op. cit., 2013.

would have tracked down the terrorists much faster. The police here use facial recognition software. They have vast databases of digitized fingerprints and DNA samples, and programs to cross-reference it all instantly against data on suspected terrorists."

Moreover, unmanned mini-drones with infrared cameras are coming on the market, and Huelin said that these were desired by Spain's anti-terrorist services; they can also record conversations. Recorded images and sounds could be analysed to identify people. "And in the case of terrorists, he said, authorities could either track their movements or pick them up." On the other hand, human intelligence was seen as necessary apart from the technology, in order to prevent terrorist attacks. A former anti-terrorism agent with Spain's Civil Guard, Luis Jimenez of the Barcelona School of Criminology, and a former Civil Guard anti-terrorist agent, pointed to the need for undercover agents, "[p]eople who can get to know different groups, communities and so on."[310]

Societal response

The immediate social response within Spain, and internationally, was to protest the attack and mourn its victims. Millions of people took to the streets in Madrid and elsewhere in Spain in massive demonstrations: "a dignified outpouring of collective grief".[311] President Aznar said, "I think that Spanish people are showing again their strength, their solidarity, and the common effort in order to overcome the atrocities of pain and terrorism."[312] However, in the aftermath of the bombings, within governmental circles and society generally, there rapidly arose a welter of controversy, contradictory blame-pinning and rumour as Spain struggled to identify the culprits and bring them to justice. Supporters and opponents of the Aznar government and its political party were bitterly divided, with many opponents outraged at what they perceived as the manipulation and concealment of the truth about the bombings for electoral advantage. The immediate electoral effect three days after the bombing was that the government's attempt to fix responsibility upon ETA and to gain political advantage against its Socialist opponents, coupled with the government's very unpopular support for American-led intervention in Iraq the year before, rebounded on it and led to defeat at the polls. Accusations and counter-accusations of political manipulation of the facts of "11M" persisted after the change of government, thus perpetuating a political polarisation that has been endemic in Spain over a very long stretch of its modern history. According to Guy Hedgecoe, whereas ETA's terrorism from 1968 onward had united the country in repudiation of terrorism, "the horror of 11M acted not to heal but to compound the country's already deep political and ideological splits".[313]

One noteworthy societal response took place the day before the election (the "day of reflection"), two days after the bombings. Sometimes called "13-M", this took the

---

[310] Ibid.

[311] Hedgecoe, Guy, "Spain's politics of memory", *openDemocracy*, 11 March 2010. http://www.opendemocracy.net/guy-hedgecoe/spains-politics-of-memory

[312] CNN.com, "Bombs were Spanish-made explosives", 13 March 2004. http://edition.cnn.com/2004/WORLD/europe/03/12/spain.blasts/index.html

[313] Hedgecoe, op. cit., 2010; see also Corera, Gordon, "The legacy of the Madrid bombings", *BBC News*, 15 February 2007. http://news.bbc.co.uk/1/hi/world/europe/6357599.stm

form of protest demonstrations in Madrid against the Aznar government by reportedly thousands of autonomous and left-wing activists. Cristina Flesher Fominaya's ethnographic account and interpretation of these events draws attention to the role of pre-existing social networks in the mobilisation of a "flash mob" on "13-M". She writes, "Autonomous social movement activists used cell phones and the internet to mobilise previously established networks for a protest that quickly spread as critiques and demands they were making resonated with an important segment of public opinion".[314] Moreover, she writes that "[n]either silence nor unity characterised the demonstrations of approximately 11 million Spaniards who marched in the pouring rain that evening."[315] This analysis argues that the anti-government protest was neither totally spontaneous nor a result of Socialist party machinations, but was initiated by a "nucleus of activists who drew on contacts developed through previous mobilisations, used new ICTs to disseminate the call, and made a conscious decision to engage in civil disobedience on the day of reflection, making the protests historically unprecedented in Spain. The strength and importance of the protests, however, extend far beyond the social movement network that initiated them, and reflect public support for the protest's critique."[316]

Economic response

Of relevance to resilience is the assertion that Spanish tourism industry interests made two months following "11M", that the tourist industry was in "excellent health". Given that tourism constitutes 12 per cent of Spain's Gross Domestic Product (GDP), the importance of demonstrating such buoyancy is highly relevant to an assessment of post-event resilience, although it reflects an outsiders' perception of the security and safety of the country or city rather than attesting to the morale of the inhabitants themselves. Nonetheless, Madrid's head of finance and tourism development, Miguel Angel Villanueva, told an international tourism conference that Madrid's catastrophe emergency plan worked effectively on the day of the bombings, and that Madrid set an example of "solidarity, respect and a level head in bad times…a coordinated, effective disciplined city that has excellent public services". Drawing attention to "spontaneous demonstrations of solidarity and protest in every workplace at public institutions and private organizations", he claimed that "our city has recovered its normality". Villanueva reported that the new security measures "not only restored normal life within the city, but are also turning Madrid into one of the safest cities in the world".[317]

This economically motivated public-relations reassurance, that Madrid had been restored to normality, ostensibly testifies to the city's resilience. Independent assessment of this, as well as further evidence of the effect of "11M" on Spain's (or Madrid's) economy, would be necessary to validate the tourist industry's claim. Some prima facie evidence bears out the assertion: the number of international visitors to Spain in 2004 increased 2.8 per cent over 2003, and in 2005 increased again by 5.5

[314] Flesher Fominaya, Cristina, "The Madrid bombings and popular protest: misinformation, counterinformation, mobilisation and elections after '11-M'", *Contemporary Social Science*, Vol. 6, No. 3, 2011, pp. 289-307, [p. 289].
[315] Ibid., p. 296.
[316] Ibid., p. 291.
[317] TravelVideo.TV, "Spain tourism in excellent health despite Madrid bombing", *TravelVideo.TV*, 3 May 2004.
http://www.exceltur.org/excel01/contenido/portal/files/MAY_04_093.pdf

per cent. For Madrid itself, the percentage growth in 2004 was 10.7.[318] Whether this provides evidence of the efficacy of an increase in surveillance as central to this "bounce-back" is far less certain.

Critical conclusions from an IRISS perspective

The history of separatist terrorism in Spain and its effects on institutions and society is the immediate background against which the events of "11M" must be seen, but the deeper background of the Franco regime is also relevant to an assessment of the salience of surveillance. It cannot be said that the combined background was one of stresses caused by the long history of dictatorial and then terrorist activity that preceded the shock of 2004, such that the latter represents "merely" one more event. A better interpretation is that the unprecedented scale of the Madrid bombing, as well as its non-ETA Islamist source, made it the decisive, qualitatively different and shocking event that should be taken as the watershed for assessing resilience.

Spain had for several decades, experienced terrorist attacks by Basque separatists, who were first thought to be implicated in the Madrid bombings. The nature of the sporadic and largely limited scope of ETA terrorism over the years– but becoming less frequent – can be said to have tested the resilience of the Spanish population, and that social life had not buckled: indeed, ETA had become a highly unpopular organisation in Spanish and Basque political life.[319] "11M", in contrast, caused a shock to the country that was also felt in many other democratic countries round the world. It came just a few years following the "9/11" events in the US, which itself had heightened fears of terrorist attack and had brought about a tightening of security measures to foil terrorism and to detect those responsible for perpetrating it.

On the other hand, "11M" and its aftermath in Spain must be seen in the light of Spain's history of Fascist and post-Fascist deep cleavages and controversies – including divisiveness over Basque separatist aspirations – that have resurfaced. They colour accounts and interpretations of the events and their subsequent social and political repercussions, and make assessments of resilience more complex and indeterminate. As Galdon Clavell et al. note, Spanish society had certainly experienced significant surveillance in the years prior to 2004. They refer to the distant past of "a dictatorship during which the day-to-day surveillance of people's political activity and affiliation continued until 1975, a consequent generalized concern over the excesses of State intervention in private and political activities in the years after the dictator's death [in 1975], and the continued activities over the last 50 years of several armed terrorist movements (the ETA being the most well-known)."[320]

---

[318] O'Connor, Noëlle, Mary Rose Stafford and Gerry Gallagher, "A chronological review of the tourism industry's reactions to terrorist attacks, using Bali (2002), London (2005), Madrid (2004) and New York (2001) as case studies", 2008. http://pc.parnu.ee/~htooman/EuroChrie/Welcome%20to%20EuroCHRIE%20Dubai%202008/papers/A%20chronological%20review%20of%20the%20tourism%20industry.pdf; see also Browne, David, "Spain bounces back from Madrid bombings", *TravelMole*, 3 June 2013. http://www.travelmole.com/news_feature.php?news_id=100439

[319] Wikipedia, *ETA*, http://en.wikipedia.org/wiki/ETA. Among the sources cited by Wikipedia are opinion polls and election results.

[320] Galdon Clavell, Gemma, Lohitzune Zuluoga Lojo and Armando Romero, "CCTV in Spain: An Empirical Account of the Deployment of Video-Surveillance in a Southern-European Country", in C.

Memory of the Franco dictatorship and its extensive surveillance lived on, but in the new democratic era that ensued, the decades of surveillance and security activities undertaken by law-enforcement and counter-terrorism agencies against separatist agencies were – like the terrorism itself – perhaps more confined and less systematic, intimidating or effective than in the Fascist period.

It is nevertheless difficult to assess the extent to which Spain has manifested resilience to adverse events (e.g., terrorism) in the wake of "11M". The increased surveillance following the bombings may in itself be evidence of state resilience in the face of heightened danger, but without deeper research it is hard to determine what the Spanish population feels about heightened surveillance in their daily lives; however, opinion polls conducted in the later 2000s appear to register strong public support for CCTV, although subject to fluctuation.[321] If there was an "exponential growth"[322] in the use of CCTV in the late 2000s, this may reflect a previous low baseline of video surveillance, but CCTV is only one of the instruments of surveillance available to states and their security and law-enforcement agencies.

One can speculate that a weakened and dwindling ETA declared its cessation of armed struggle in 2011 in part as a result of increasingly effective state surveillance and intelligence activities in the 2000s, starting even after "9/11" and accelerating after "11M". However, little can be said with any certainty about this, or about general Spanish resilience to surveillance either pre- or post-"11M". If the longer-term effect of "11M" is that of a further excuse for an "enduring struggle over the country's past"[323], it is ironic that the resilient "bounce-back" is to a continuous, deeply-rooted and tragic socio-political polarisation rather than to the confident, unified national solidarity portrayed in some other countries in the aftermath of a major adverse event. Flesher Fominaya remarks: "The acute division in public opinion over responsibility for the bombings reflects the deep left-right cleavage in Spain."[324] She underlines "the importance of political flash mobs as a means of countering increased surveillance and repression of social movements in a post-9/11 security context…while at the same time not romanticising the possibilities of new ICTs: security forces can and do bring down cell phone networks as a means of social control, even in democratic countries".[325]

William R. Webster, Eric Töpfer, Francisco Klauser and Charles D. Raab (eds.), *Video Surveillance: Practices and Policies in Europe*, IOS Press, Amsterdam, 2012, pp. 133-144 [p. 134].

[321] Cited in Galdon Clavell, Gemma, Lohitzune Zuluoga Lojo and Armando Romero, "CCTV in Spain: An Empirical Account of the Deployment of Video-Surveillance in a Southern-European Country", in C. William R. Webster, Eric Töpfer, Francisco Klauser and Charles D. Raab (eds.), *Video Surveillance: Practices and Policies in Europe*, IOS Press, Amsterdam, 2012, pp. 133-144 [pp. 140-141].

[322] Galdon Clavell, Gemma, Lohitzune Zuluoga Lojo and Armando Romero, "CCTV in Spain: An Empirical Account of the Deployment of Video-Surveillance in a Southern-European Country", in Webster, C. William R., Eric Töpfer, Francisco Klauser and Charles D. Raab (eds.), *Video Surveillance: Practices and Policies in Europe*, IOS Press, Amsterdam, 2012, pp. 133-144 [p. 134].

[323] Hedgecoe, Guy, "Spain's politics of memory", *openDemocracy*, 11 March 2010. http://www.opendemocracy.net/guy-hedgecoe/spains-politics-of-memory

[324] Flesher Fominaya, Cristina, "The Madrid bombings and popular protest: misinformation, counterinformation, mobilisation and elections after '11-M'", *Contemporary Social Science*, Vol. 6, No. 3, 2011, pp. 289-307 [p. 305, note 5].

[325] Flesher Fominaya, op. cit., 2011 [p. 304].

3.2.3 The London bombings, 2005 ("7/7")

Dr Richard Jones and Professor Charles Raab, University of Edinburgh

Nature of the adverse event

At 8:50 on 7 July 2005, the morning after Londoners had celebrated the announcement that their city was to host the Olympic Games in 2012, and while Prime Minister Tony Blair was hosting a G8 meeting of world leaders at Gleneagles in Scotland amid tight security, three bombs were detonated on the London Underground railway. Just an hour later, at 9:47, a fourth bomb was detonated on a London double-decker bus. A total of 56 people were killed, and 775 were injured. Each of the four bombs was detonated by a suicide bomber, and all of the bombers "were British citizens resident in the UK".[326] The terror attack inflicted the greatest number of casualties on Londoners in a single attack since World War II[327] and "the first instance of suicide bombings in Western Europe in contemporary times".[328]

The immediate concern of the emergency services was to respond to the attack scenes, though mindful of the possibility that further bombs might be detonated. Subsequent reviews as to how well the emergency services coped with the unfolding events vary as to their assessment (see below), but in general the response seems to have been quick and efficient. Still, "[t]hose in the bombed underground trains were not reached by the emergency services immediately, and were left in the dark, with few announcements, and no way of knowing whether they would be rescued, or whether the rail lines were live" with electricity.[329]

One might characterise the London bombings as a major shock event invoking emergency services and governmental contingency measures, occurring against the background of various stressors borne of international relations, given the UK's affiliation with US and European involvement in conflicts in the Middle East, and given London's political symbolism and its crowded populace. If the nature of the attack was cruel, fatal and bloody, it nevertheless lacked the audacity of the 9/11 attacks, and was less deadly than the Madrid bombings. On the other hand, what did come as a shocking surprise both for the British public and seemingly for the British intelligence community was that the bombers turned out to be British nationals, and that Al-Qaida's appeal and reach were clearly far closer to home than previously thought.

Psychologically, the bombings seem to have been experienced by many locals as stressful. A research study, involving a telephone survey of 1010 English-speaking

---

[326] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, Cm 6785, London, The Stationery Office Limited, 2006, p. 28.
[327] Aylwin, Christopher J., Thomas C König, Nora W Brennan, Peter J Shirley, Gareth Davies, Michael S Walsh and Karim Brohi, "Reduction in critical mortality in urban mass casualty incidents: analysis of triage, surge, and resource use after the London bombings on July 7, 2005", *The Lancet*, Vol. 368, December 23/30, 2006, pp. 2219-2225 [p. 2219].
[328] Segell, Glenn M., "Terrorism on London Public Transport", *Defense & Security Analysis*, Vol. 22, No. 1, 2006, pp. 45-59 [p. 53].
[329] Drury, John, Chris Cocking and Steve Reicher, "The Nature of Collective Resilience: Survivor Reactions to the 2005 London Bombings", *International Journal of Mass Emergencies and Disasters*, Vol. 27, No. 1, March 2009, pp. 66-95 [p. 71].

adult Londoners conducted between 18-20 July 2005 to try to determine levels of stress and travel patterns among city residents almost two weeks after the bombings[330] found that "31% of respondents reported substantial levels of stress" and while the majority displayed a certain resilience saying that "the bombings would have no impact on their travel plans", about a third said they would use public transport less and go into central London more rarely. An interesting finding was that three-quarters of respondents had tried to contact family or friends in the immediate aftermath of the attacks, and those who had experienced difficulties in speaking to loved ones on their mobile phones (the cellular network was heavily congested and disrupted on the day) "were also significantly more likely to experience substantial stress". It should be noted, however, that although the survey sample size was fairly large it represented a low response rate of about only 10% of the some 11,000 people originally contacted.

In a follow-up study by the same research team seven to eight months later, the 31% rate experiencing "substantial stress" "had fallen to 11%" – which, the authors note, while "considerably reduced…is not a trivial figure". [331] In this second study, "perceived threat to 'close family members or those dear to you' was more persistent" than "perceived threat to self", suggesting that "the medium-term psychological impact of a terrorist incident is largely mediated by the perceived risk to one's family rather than to oneself". Interestingly, not all psychological consequences of the attacks were entirely negative, with some separate positive changes also occurring, and "nearly 80% of participants who reported changes in self-perception in this study reported that these changes were at least partially positive; moreover, 45% of those who said they saw the world differently saw it at least somewhat more positively than before".[332]

Institutional response

In the immediate aftermath of the Tube and bus explosions, the emergency services sprang into action following a "well-rehearsed drill" ("Gold Command") for just such a contingency. Indeed, a practice exercise involving medics and the emergency services had been held not far from the location of the bombings just a few weeks earlier on 12 June.[333] London has a 'major incident plan…developed and organised by the London Emergency Services Liaison Panel'.[334] However, the three Tube bombs exploded deep underground, there was no mobile phone signal there, and hospitals awaiting casualties had no idea as to how many patients to expect. This was clearly a

[330] Rubin, G. James, Chris R. Brewin, Neil Greenberg, John Simpson and Simon Wessely, "Psychological and behavioural reactions to the bombings in London on 7 July 2005: cross sectional survey of a representative sample of Londoners", *British Medical Journal*, doi:10:1136/bmj.38583.728484.3A, pp. 1-7, [pp. 1, 6]

[331] Rubin, G. James, Chris R. Brewin, Neil Greenberg, Jamie Hacker Hughes, John Simpson and Simon Wessely, "Enduring consequences of terrorism: 7-month follow-up survey of reactions to the bombings in London on 7 July 2005", *British Journal of Psychiatry*, Vol. 190, 2007, pp. 350-356 [pp. 353, 354].

[332] Ibid.

[333] Segell, Glenn M., "Terrorism on London Public Transport", *Defense & Security Analysis*, Vol. 22, No. 1, 2006, pp. 45-59 [p. 47].

[334] Aylwin , Christopher J., Thomas C. König, Nora W. Brennan, Peter J. Shirley, Gareth Davies, Michael S. Walsh and Karim Brohi, "Reduction in critical mortality in urban mass casualty incidents: analysis of triage, surge, and resource use after the London bombings on July 7, 2005", *The Lancet*, Vol. 368, December 23/30, 2006, pp. 2219-2225 [p. 2220].

major attack, however, and "[o]ver 100 ambulance vehicles and more than 250 ambulance staff attended the incident scenes", two central London hospitals "were placed on full emergency status", and the helicopter "air ambulance" brought in "additional medical staff from outside London" and "was also able to fly in 31 doctors and paramedics to the four bomb sites". [335] Doctors arrived relatively quickly at the four scenes. "Working conditions" for the doctors treating the injured and identifying the dead on the underground trains were described as "difficult" or "poor", often "dark" and messy. Doctors reported that "[c]ommunications were difficult between the scenes and ambulance control because all but one mobile telephone network failed and radio communications were also very difficult" as they did not work underground at all.[336] (The subsequent Report of the London Assembly's Review Committee offered a less diplomatic assessment of the same issue.[337]) Still, many of the doctors involved had experience of working underground, and the dead were quickly identified and the injured treated on site or "evacuated to the surface", and overall the "critical mortality rate of 15%" was low.[338]

As the medical response was underway, the police and media response was to try to understand what had happened; manage security on London streets and on its public transport; advise the London public on what to do (at that point it was unclear whether further bombs would be detonated); and to try to catch the bombers before they could strike again (it was not yet known that the attackers had been suicide bombers).

The police part of Gold Command is led by the Commissioner of the Metropolitan Police, who also reports to the UK Government's COBRA emergency committee, which is chaired by the Prime Minister and includes the Security Services (MI5). The Committee was convened on the day of 7 July "and decided that there was no need to involve the armed forces" and that "[b]y the following morning all bus routes were operating normally. Similarly, almost 80 per cent of the Underground system was operating, with the exception of those areas that were still under forensic investigation".[339] During the day, Prime Minister Tony Blair announced at the G8 meeting that there had been a terrorist attack, before returning to London, though "the summit continued without him. Similarly, the Mayor of London, Ken Livingstone, was in Singapore for the Olympic Committee's decisions and his Deputy took charge for ground co-ordination". Senior staff from the emergency services and from London Underground gave press conferences and briefed journalists "at the QE2 Conference Centre adjacent to the Houses of Parliament"; TV news gave extended live coverage throughout the day; and "a support center for victims and relatives was set up at the Queen Mother Sports Centre", also nearby. Additionally, "[t]he casualty bureau, set up to help people locate family members and friends, took 104,000 calls within the first 24 hours". "The first lead" in the police investigation in fact came not from the police themselves but after "the family of one of the bombers (19-year-old Hasib Hussain) reported him missing on the night of the bombing". Analysis of "CCTV

[335] Segell, Glenn M., "Terrorism on London Public Transport", *Defense & Security Analysis*, Vol. 22, No. 1, 2006, pp. 45-59 [p. 48].
[336] Lockey, D.J., R. MacKenzie, J. Redhead, D. Wise, T. Harris, A. Weaver, K. Hines and G.E. Davies, "London bombings 2005: The immediate pre-hospital response", *Resuscitation*, Vol. 66, 2005, pp. ix-xii [pp. x, xi].
[337] London Assembly Review Committee, *Report of the 7 July Review Committee*, London Assembly, London, June 2006, p. 120.
[338] Aylwin et al, op. cit, 2005, p. 2224.
[339] Segell, op. cit., 2006, pp. 47, 49.

evidence revealed that they had travelled to Luton in rental cars from the city of Leeds, which is 230 miles north of London, to meet the fourth bomber. These three terrorists were Muslims of Pakistani origin …. The fourth terrorist bomber was [a] Jamaican-born 19-year-old… Muslim convert".[340] All four were British citizens and lived in the UK.

Two further events are also worth mentioning here; although they could perhaps be classed as additional "adverse events" themselves, they are perhaps best understood within the context of the police and institutional responses to the "7/7" attacks discussed above. The first is that a second series of bombings were attempted (though failed) on 21 July 2005, exactly two weeks after the "7/7" bombings, again by Muslims who were British citizens. The men unsuccessfully attempted to set off bombs they were carrying in rucksacks. All the men were arrested just a few days later, but the second attacks served to put the authorities on a very high state of alert. The second event of note is the fatal shooting of an innocent Brazilian man, Jean Charles de Menezes, by armed police at a London Underground station on 22 July, mistakenly identified by the police and surveillance teams as one of the terror suspects they were hunting following the attempted bombings the day before, and who they believed was about to try again to detonate a suicide bomb. Despite several official responses to the shooting, including an official inquiry and an inquest, criminal charges against the Metropolitan Police Service (though collectively, not against individual officers, and oddly under Health and Safety legislation), the exact circumstances surrounding the shooting remain unclear. However, it does appear that there were surveillance and communication failures on the part of the different police and security teams working together on the day of the shooting.

The seeming immediacy of the threat at the time, the fact that the terror threat was found to have arisen from within British society rather than from outside it, allied perhaps with the intensity and immediacy of the media coverage of the attacks (see below), gave rise to a raft of further surveillance, policing, legal and counter-terrorism strategy responses.

In a discussion of "surveillance and counterterrorism in London", Pete Fussey has argued that while "[s]urveillance technologies are increasingly introduced and legitimized in terms of counterterrorism, and this association is routinely projected onto the public consciousness through such occurrences as the posthumous closed-circuit television (CCTV) footage of the London suicide bombers following July 7, 2005", though the reality of their use casts doubt on their practical effectiveness. For example, in the case of "7/7", CCTV cameras did not appear to deter nor help police in real-time co-ordination against the attacks, and "CCTV had only the most marginal of roles in the identification of the four bombers".[341] Fussey notes too how "the camera fitted aboard the bus blown up by Hasib Hussein near Tavistock Square on July 7, 2005, was not working (and had not been working for a number of weeks prior to the attack)". A year later, however, the Official Report into the bombings noted that as part of the police investigation, "more than 6,000 hours of CCTV footage were

[340] Segell, op. cit., 2006, pp. 48-49, 50, 52-53.
[341] Fussey, Pete, "Observing Potentiality in the Global City: Surveillance and Counterterrorism in London", *International Criminal Justice Review*, Vol. 17, No. 3, 2007, pp. 171-192 [p. 182].

being examined".[342] On the other hand, the House of Commons official report on the bombings later detailed how the bombers had been caught on numerous CCTV cameras en route on the morning of the bombings, and which had helped piece together a detailed and accurate picture of their movements, at least on that day.[343] Accounting for the UK security authorities' continued push toward widespread usage of CCTV, Fussey suggests that this be understood as part of a move toward a technological and convergent social control strategy, and the conjoining of previously discrete crime control and counter-terrorism measures – citing, for example, Haggerty and Ericson's "surveillant assemblage" thesis, and Haggerty and Gazso's variant on the same acknowledging the system-absorption of user-generated media (e.g., camera-phone images).[344] The danger of such technocratic surveillant expansionism, according to Fussey, is not merely that technical surveillance systems are likely to be less effective in practice in countering terrorism than, for example, human intelligence, but that "some groups may find themselves catalogued within samples of suspicion and hence 'overpoliced'."[345]

Attempting to learn from events and to assess both the immediate response to the bombings and whether there had been prior intelligence failings, both the House of Commons and the Government's Intelligence and Security Committee published reports in May 2006. The House of Commons report produced a detailed time-line reconstructing events, reviewed the backgrounds of the bombers, noted the bombers' stated motives as a response to overseas conflicts, and found that it was not known if the bombers had been directed from Overseas.[346] The Intelligence and Security Committee Report focused in greater detail on intelligence and security aspects, including considering whether there had been any intelligence failings, and whether lessons could be learned. The Report noted that by 2005, the number of "primary investigative targets" (i.e., possible terrorist suspects) in the UK had risen to 800, outstripping MI5's surveillance capability. None of the four bombers had been identified as potential terrorists, though two had been identified "on the peripheries of other investigations". Among the Report's findings were that better intelligence coverage of certain overseas countries was required and that "the radicalisation of British citizens were not fully understood or applied to strategic thinking".[347] In May 2009, the Intelligence and Security Committee produced a further Report[348], and

---

[342] Bulley, Dan, "'Foreign' Terror? London Bombings, Resistance and the Failing State", *British Journal of Politics & International Relations*, Vol. 10, 2008, pp. 379-394 [p. 381]; House of Commons, *Report of the Official Account of the Bombings in London on 7th July 2005*, HC 1087, The Stationery Office, London, 2006, p. 26.

[343] House of Commons, *Report of the Official Account of the Bombings in London on 7th July 2005*, HC 1087, The Stationery Office, London, 2006, pp. 2-5.

[344] Fussey, Pete, "Observing Potentiality in the Global City: Surveillance and Counterterrorism in London", *International Criminal Justice Review*, Vol. 17, No. 3, 2007, pp. 171-192, p. 185; Haggerty, Kevin, and Richard Ericson, "The surveillant assemblage", *British Journal of Sociology*, Vol. 51, No. 4, 2000, pp. 605-622; Haggerty, Kevin, and A. Gazso, "Seeing beyond the ruins: Surveillance as a response to terrorist threats", *Canadian Journal of Sociology*, Vol. 30, No. 2, 2005, pp. 169-187.

[345] Fussey, op. cit., 2007, p. 188.

[346] House of Commons, *Report of the Official Account of the Bombings in London on 7th July 2005*, HC 1087, The Stationery Office, London, 2006.

[347] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, Cm 6785, The Stationery Office Limited, London, 2006, pp. 8, 13-14, 43.

[348] Intelligence and Security Committee, *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, Cm 7617, The Stationery Office Limited, London, 2009.

which (as with the other Reports discussed above) can be seen to be part of the institutional response. This Report included a significant amount of description of police and intelligence agents' surveillance of various terrorist suspects, giving a sense of the volume and complexity of material with which they had to grapple, even if much operational detail is redacted for security reasons.

It was unclear about whether the UK suspects were being "directed" or supported from abroad. Phythian quotes John Gray as arguing that,

> There may no longer be anything resembling a globally organised terrorist network, but by instantaneously disseminating the same images of carnage and panic throughout the world, the media have globalised our perception of terror. Governments behave as if this media apparition were an actual entity, with the result that the policies that are adopted in order to resist terrorism are ineffective and sometimes disastrously counter-productive.[349]

The UK's CONTEST counter-terrorism policy was originally launched in 2003 as a way of co-ordinating the UK Government's various responses to terrorism in the light of the "9/11" attacks in the US in 2001.[350] The policy has been revised and expanded since, "funding has increased from £6 million per year in 2006 to £140 million in 2008/9"[351], and contains four elements – arguably recognisable as different aspects of "resilience":

> The Government's counter-terrorism strategy, known as CONTEST, is divided into four "strands" or "workstreams": Pursue; Prevent; Protect; and Prepare. The essence of these strands is defined by the Government as:
>
> - Pursue: to stop terrorist attacks;
> - Prevent: to stop people becoming terrorists or supporting violent extremism;
> - Protect: to strengthen our protection against terrorist attacks, and
> - Prepare: where an attack cannot be stopped, to mitigate its impact.[352]

The UK's main intelligence agencies (MI5, MI6 and GCHQ)[353] contribute to all of the strands, including providing "input to risk assessments that underpin the resilience and response capabilities being developed".[354] The strands of this approach that appear closely related to a "resilience" approach—namely Pursue, Protect and Prepare—have been fairly uncontroversial. However, the same cannot be said of the Prevent strand.

---

[349] Gray, John, "A Violent Episode in a Virtual World", *New Statesman*, 18 July 2005, p. 16; cited in Phythian, Mark, "Intelligence, policy-making and the 7 July 2005 London bombings", *Crime, Law and Social Change*, Vol. 44, 2005, pp. 361-385 [p. 371-372].

[350] House of Commons Home Affairs Committee, *Project CONTEST: The UK Government's Counter Terrorism Strategy*, Report HC 212, The Stationery Office Limited, London, 7 July 2009, p. 3.

[351] Briggs, Rachel, "Community engagement for counterterrorism: lessons from the United Kingdom", *International Affairs*, Vol. 86, No. 4, 2010, pp. 971-981 [p. 971].

[352] House of Commons Home Affairs Committee, *Project CONTEST: The UK Government's Counter Terrorism Strategy*, Report HC 212, The Stationery Office Limited, London, 7 July 2009, pp. 8-9.

[353] MI5 (formally known as the Security Service) is responsible for domestic intelligence and national security. MI6 (formally referred to as the Secret Intelligence Service, or SIS) provides intelligence from abroad. GCHQ (the Government Communications Headquarters) provides signals intelligence through monitoring and intercepting communications, and contains a branch named CESG tasked with helping secure critical national infrastructure.

[354] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, Cm 6785, The Stationery Office Limited, London, 2006, p. 5.

Exactly what is involved in the Prevent strand remains a little unclear, but it seems designed to foster better relations between police and Muslim communities, in part to generate more trust and in part to generate better intelligence. However, these aims sit uneasily together. Briggs identifies four possible "[rationales] for community engagement in counterterrorism".[355] First, "if terrorists are well integrated, communities may be able to act as an early warning system for the police and intelligence services". Second, communities can try to prevent radicalisation, especially among the young. Third, communities can address injustices and grievances that may otherwise "allow terrorists' messages to resonate more widely". Last, the "police and Security Service" are likely to be more effective if they act in "partnership" with "Muslim communities". [356]

In July 2011, the third version of the CONTEST strategy was published, the revisions in part due to criticisms that some earlier aspects of, and spending on the strategy were not effective. Anecdotal evidence suggests that the Prevent strategy, possibly in conjunction with communications surveillance, may be "successful" to some degree, in helping identify potential suspects and drawing these to the attention of the Security Service. However, this generates a large list of names, and a potentially huge volume of data, and the problem then becomes how to establish which individuals represent actual potential threats. The problem of the "'clean terrorist'" (a person with no prior record but who goes on to commit a terror act) thus exists at two levels: the first is where there truly is no prior intelligence record on the individual; the second is where the person was known by intelligence agencies but was not considered sufficiently important to warrant an (extremely expensive and resource-intensive) surveillance operation. As Gregory noted in 2005, "[i]t is obvious from the many accounts in the press of circumstances leading to arrests and from court evidence that the *sigint* [i.e., surveillance of electronic communications] work of GCHQ, MI5 and MI6 is making a major contribution to disruption and dismantling operations against those suspected of terrorist offences. However, older, traditional methods of penetration and the management of human intelligence sources are also being used although of course one cannot expect to find confirmed details of these." [357]

The *Prevent* policy remains controversial, however, and it has been argued that "the experiences of Muslim communities" have become those of being "suspect communities". [358] Briggs notes that some Muslims have been "subject to physical and verbal attacks because of their religion. Muslims also feel indiscriminately targeted by anti-terrorist laws."[359] Kundnani argues that the policy "has undermined many progressive elements within the earlier community cohesion agenda and absorbed

---

[355] Briggs, Rachel, "Community engagement for counterterrorism: lessons from the United Kingdom", *International Affairs*, Vol. 86, No. 4, 2010, pp. 971-981 [pp. 972-974].
[356] Ibid.
[357] Gregory, Frank, "Intelligence-led Counter terrorism: A Brief Analysis of the UK Domestic Intelligence System's Response to 9/11 and the Implications of the London Bombings of 7 July 2005", *Area: International Terrorism – ARI no. 92/2005*, Real Instituto Elcano de Estudios Internacionales y Estrategicos, 2005, pp. 1-5 [p. 2]. http://www.realinstitutoelcano.org/analisis/781/Gregory781-v.pdf
[358] Spalek, Basia, and Robert Lambert, "Policing within a counter-terrorism context post-7/7: The importance of partnerships, dialogue and support when engaging with Muslim communities", in Roger Eatwell and Matthew J. Goodwin (eds.), *The New Extremism in 21st Century Britain*, Routledge, London, 2010, pp.103-121 [p.106].
[359] Briggs, Rachel, "Community engagement for counterterrorism: lessons from the United Kingdom", *International Affairs*, Vol. 86, No. 4, 2010, pp. 971-981 [p. 979].

from it those parts which are most problematic".[360] Hussain and Bagguley argue that British Muslims have effectively become "securitized", in the sense of "it [becoming] 'common sense' that [they] represent a threat", generating "public support enabling exceptional state actions, and new legislation".[361]

Legal response

Perhaps the most notable legal response to the London bombings was the Terrorism Act 2006. The Bill was introduced in October 2005, and received Royal Assent (i.e., became an Act of Parliament) on 30 March 2006. The origins of the Act in fact date to just over a week after the London bombings, when the then Home Secretary Charles Clarke wrote to representatives of opposition parties indicating the (Labour) Government's intention to propose new anti-terror legislation, based on ideas being considered before the bombings, and seeking cross-party consensus. The Act introduces various new offences relating to the preparation of terror attacks, such as training for a terrorist act. Such provisions may appear uncontroversial, but nevertheless mean that it became an offence simply to train (for example), even if the person did not in fact go on to carry out any such terror act. More obviously controversial, and more clearly at odds with the Labour Government's prior commitment to human rights protections, were the provisions relating to "encouragement of terrorism" including criminalising the "glorifying" of terrorism (which thus seems to limit freedom of political expression); and the extension of the period during which a terrorist suspect could be detained without charge. It was the latter that drew most criticism, the Government initially proposing that that time period be extended from the then limit of 14 days to a new maximum of 90 days. Some senior police officers publicly supported the proposed extension, arguing it was necessary for various practical reasons relating to terror investigations. Critics of the provision argued that the measure was illiberal, dangerous and reminiscent of the notorious "internment" provisions that the British Government had used to detain Irish Republican terrorist suspects in Northern Ireland in the 1970s, and which ultimately many felt to have been counter-productive as well as repressive. In the event, Parliament rejected the 90 days proposal, and instead passed an amendment increasing the detention limit to 28 days.

Whether such an extension (to almost a month) represents a worrying move towards a more authoritarian state, or whether instead Parliament's rejection of the initial proposal allowing terror suspects to be detained without charge for three months demonstrates the "resilience" of UK liberal Parliamentary democracy, has been the subject of debate. While not discussing the Act directly, Abbas sketches a wider context of policing in which, even before the London bombings, "large numbers of innocent Muslims were being arrested, questioned and released without charge. In the post-7/7 period, this pattern has remained if not intensified."[362] Pantazis and Pemberton argue that the 2006 anti-terror legislation was consistent with a wider pattern in anti-terror laws introduced since 9/11, in which Muslims were effectively

[360] Kundnani, Arun, *Spooked: How Not to Prevent Violent Extremism*, Institute of Race Relations, London, 2009.
[361] Hussain, Yasmin, and Paul Bagguley, "Securitized citizens: Islamophobia, racism and the 7/7 London bombings", *The Sociological Review*, Vol. 60, 2012, pp. 715-734 [p. 716].
[362] Abbas, Tahir, "Muslim Minorities in Britain: Integration, Multiculturalism and Radicalism in the Post-7/7 Period", *Journal of Intercultural Studies*, Vol. 28, No. 3, August 2007, pp. 287-300 [p. 294].

constituted as a "suspect community" (a term originally coined by Hillyard to capture the effect, as he saw it, of earlier UK anti-terror legislation, in relation to Irish people and Irish Republican terrorism).[363] The authors conclude that "The construction of the Irish as a suspect community through the PTA served to radicalize and alienate, and, ultimately prolong the Irish conflict. The lessons of this conflict are largely not being heeded.… As we have demonstrated, the 'terror of prevention' continuum, which ranges from the day-to-day harassment of Muslims through stop and search to high-profile police raids, has had a corrosive effect on the relations between Muslim communities and the police. Within this context, the conditions for radicalization are being fomented and the 'flow of information' necessary for effective counter-terrorism policing has been jeopardized. Thus, the very powers that are supposed to promote security are serving to undermine it, whilst Muslim communities continue to endure the spectre of state suspicion." Greer has strongly challenged this thesis, offering a wide-ranging critique, arguing that "[t]here is no evidence to support it, and a great deal that points in the opposite direction".[364]

Discussing the passing of the Terrorism Act 2006, Vermeule argues that the passage of the Bill and the limiting by the legislature of the executive's initial attempt to increase police powers suggests that legislatures can prove effective at "substantially [reining in] executive proposals".[365] Along similar lines, Waddington argues that while the British government "*has* reacted to the threat of jihadism by introducing legislation and changes in police practice that have eroded civil liberties…this has *not gone uncontested*".[366] Indeed, "the obvious conclusion" is Parliamentary and judicial challenges to "anti-terrorist policies represents success for the civil libertarian cause and political frustration is evidence of that".[367]

Societal response

The UK societal response to the "7/7" London bombings appears varied and mixed, and involved numerous different actors, accounts, political debates, media representations, public attitudes and academic studies (a number of which are cited here).

Research on civil contingencies and disasters reveals that "the notion of mass panic has been largely discredited by the finding of orderly, meaningful mass behavior in disasters", even if architects, social policy-formers and popular culture still subscribe to the assumption of mass panic. "If people are naturally collectively resilient, however, rather than being treated as part of 'the problem', crowds can be trusted with information during emergencies…and communities should have greater

[363] Pantazis, Christina, and Simon Pemberton, "From the 'Old' to the 'New' Suspect Community: Examining the Impacts of Recent UK Counter-Terrorist Legislation", *British Journal of Criminology*, Vol. 49, 2009, pp. 646-666 [pp. 661-662]; Hillyard, Paddy, *Suspect Community: People's Experiences of the Prevention of Terrorism Acts in Britain*, Pluto Press, London, 1993.
[364] Greer, Steven, "Anti-terrorist Law and the United Kingdom's 'Suspect Muslim Community: A Reply to Pantazis and Pemberton", *British Journal of Criminology*, Vol. 50, 2010, pp. 1171-1190 [p. 1171].
[365] Vermeule, Adrian, "Emergency Lawmaking after 9/11 and 7/7"*, The University of Chicago Law Review*, Vol. 75, 2008, pp. 1155-1190 [p. 1190].
[366] Waddington, P.A.J., "Terrorism and Civil Libertarian Pessimism: Continuing the Debate", *Policing & Society*, Vol. 16, No. 4, 2006, pp. 415-421 [p. 418].
[367] Ibid.

involvement in the own defence and psychological recovery." Different theoretical models of orderliness in emergency crowds have been proposed, including one based on the notion of "*mass emergent* sociality or *collective* resilience, i.e. coordination and cooperation with a crowd of *strangers*". A retrospective study of the behaviour of survivors in the immediate aftermath of the London attacks, based on an analysis of eye-witness accounts, found "selfish" behaviours to be rare and "helping" behaviours to be more common. Examples included accounts of people "pulling people from the wreckage, and holding people up as they evacuated". Yet many survivors also report fearing they would die; this may in turn have generated a sense of shared predicament, and hence social unity, leading to helping behaviours. The study's authors conclude that "a notion of resilience in unstructured crowds is necessary to counter the currently dominant vulnerability framework".[368]

Two weeks after the bombings, a group of medics and representatives of various stakeholders met as a "Psychosocial Steering Group" under the auspices of the London Development Centre for Mental Health and subsequently successfully applied for UK Government funding for a "screen and treat approach", to identify victims of the bombings with mental health problems and to offer appropriate psychological treatment. Although people are often psychologically resilient and "most psychological responses to trauma are short-term and resolve naturally", others may be deeply affected by their experiences (often suffering from Post-Traumatic Stress Disorder; a small minority may suffer from travel phobia specifically instead[369]), yet only a few will seek out treatment. Only 14 survivors of the bombings were referred for counselling directly by their own doctors, whereas the more pro-active "screen and treat" outreach programme identified no fewer than "255 bombing survivors with mental health problems severe enough to require treatment".[370] Another study found that survivors suffering from PTSD reported a sense of togetherness with other victims immediately after the attacks, but a sense of social disconnection post-7/7; yet even they often "displayed resilience through their determination to rebuild their lives at an intimate level".[371]

Terrorist attacks are also known to have psychological effects on the wider population, though these effects are ameliorated by individuals' psychological resilience. Research suggests that, "[r]emarkably, individuals confronted with a terrorist threat seem to display high levels of psychological resilience", where "*resilience* is treated as a psychological construct referring to the ability to cope with adversity and to endure stressful situations … Resilient individuals appear to have a mechanism that enables them to identify stressful circumstances, achieve a realistic appraisal for action, and solve problems effectively. Londoners' behaviour changed after the attacks: "Retail sales fell 8.9%...shoppers and day-trippers kept their distance

---

[368] Drury, John, Chris Cocking and Steve Reicher, "The Nature of Collective Resilience: Survivor Reactions to the 2005 London Bombings", *International Journal of Mass Emergencies and Disasters*, Vol. 27, No. 1, March 2009, pp. 66-95, pp. 68, 71 (emphases in original), 78, 89.

[369] Handley, Rachel V., Paul M. Salkovskis, Peter Scragg and Anke Ehlers, "Clinically significant avoidance of public transport following the London bombings: Travel phobia or subthreshold posttraumatic stress disorder?", *Journal of Anxiety Disorders*, Vol. 23, 2009, pp. 1170-1176.

[370] Brewin, Chris R., Patricia d'Ardenne and Anke Ehlers, "Promoting Mental Health Following the London Bombings: A Screen and Treat Approach", *Journal of Traumatic Stress*, Vol. 21, No. 1, February 2008, pp. 3-8 [p. 6].

[371] Wilson, Naomi, Patricia d'Ardenne, Carleen Scott, Howard Fine and Stefan Priebe, "Survivors of the London Bombings with PTSD: A Qualitative Study of Their Accounts During CBT Treatment", *Traumatology*, Vol. 18, Issue 2, pp. 75-84 [p. 82].

from the capital…tube travel dropped substantially, by 10-15%...while bike sales increased 20% as a result of the attacks." People experiencing indirect exposure to terrorist attacks (for example, by reading or viewing media coverage) can also be affected. Studying 338 members of the public from the north-west of England who had had no direct experience of the bombings nor knew any of the victims, researchers found that psychological "resilience helped attenuate the effects of negative emotions in the months after the London attacks", and "that religious faith can also help people respond to terrorism".[372]

Bulley suggests that, "[i]n many ways, the British public's response has been encouraging", and quotes liberal newspaper columnist Jonathan Freedland as writing, "[i]n this sense, the politics of 7/7 has played strangely. It has not led to a new hawkishness in the British public" [*The Guardian*, 7 July 2006].[373] Croft contends that whereas 9/11 saw the "London elite" downplay the terror threat in the light of "concerns about the fragility of public resilience", the 7/7 attacks prompted an "'overplaying', in which a new global ideological threat, with dangers to British existence, has been brought rhetorically into being". At the same time, he argues, UK domestic counter-terror strategy looks within, content to "[play] up the otherness of the [British] Muslim community", a stance he interprets as reflective of the political classes now believing that "there is a greater resilience among society than was first thought, that panic is not as likely as perhaps it once seemed. Bluntly, 7/7 has created greater confidence in the British public."[374]

An analysis of "British Social Attitudes data collected between June and November 2005" examined "the readiness to trade off civil liberties for enhanced security", and found that after the July bombings citizens' concerns increased "significantly", with greater "willingness to trade off civil liberties for security", and moreover that "these perceptions [did] not revert to pre-attack levels". [375] This study found that "the post-attack shift in public support for security policies at the cost of civil liberties – such as freedom of speech, rights of suspects... – is sizable". Interestingly, "this shift only manifests itself a week after the attack", suggesting a possible role of the news media, television coverage or public debate. [376]

A study of "the experiences of British Pakistanis living in West Yorkshire after the 7 July bombings" based on 141 interviews found a number of interesting findings. One interviewee reported feeling people looking at them differently: "Well you would just get on the bus sometimes and you get funny looks, because you're carrying a bag, you could be just carrying a shoulder bag…". Interviewees' accounts of their identity were mixed, with British-born Pakistani Muslims identifying primarily as being British, but with "first-generation migrants" identifying more as "a Pakistani living in England",

---

[372] Bux, Shahid M., and Sarah M. Coyne, "The Effects of Terrorism: The Aftermath of the London Terror Attacks", *Journal of Applied Social Psychology*, Vol. 39, Issue 12, pp. 2936-2966 [p. 2938, emphasis in original; pp. 2939-2940; p. 2960].

[373] Bulley, Dan, "'Foreign' Terror? London Bombings, Resistance and the Failing State", *British Journal of Politics & International Relations*, Vol. 10, 2008, pp. 379-394 [pp. 379-380].

[374] Croft, Stuart, "British Jihadis and the British War on Terror", *Defence Studies*, Vol. 7, No. 3, 2007, pp. 317-337, p. 332-334.

[375] Bozzoli, Carlos and Cathérine Müller, "Perceptions and attitudes following a terrorist shock: Evidence from the UK", *European Journal of Political Economy*, Vol. 27, 2011, S89-S106, S89-S90; S101; S103.

[376] Ibid.

for example. Some "others prioritized their religious identity". Some younger, British-born interviewees described themselves as "British Muslim", with mixed (but among younger interviewees, not wholly negative) experiences of what "Britishness" meant to them. Contrary to some opinion poll surveys that found an "apparent level of support or sympathy for the London bombers among British Muslims", the study found that "interviewees were highly critical of the bombings", which were seen as "morally wrong" and as leading to "wider negative consequences for Pakistani and Muslim communities in Britain. Some did say that they could understand why the bombings were committed, but this was very different from actually supporting them." Moreover, "interviewees recalled how the bombings and the whole idea of suicide bombing as a political strategy were condemned in local mosques", and reported how the events of 7/7 had served to unify the Muslim community – interestingly, seemingly not as a communal gelling of a minority in the face of wider discrimination (even if that might have been happening) but rather as a collective response to a perceived tiny minority problem contained within. [377]

Disturbingly, a study of "racially motivated hate crimes" carried out in England "in the wake of the 7/7 terror attack that hit London in July 2005 and the 9/11 terror attack that hit the US in September 2001" found "significant increases in hate crimes against Asians and Arabs that occurred almost immediately in the wake of both terror attacks and which lasted for a prolonged period. Moreover, hate crimes against Asians and Arabs do not return back to their pre-attack levels, showing a permanent increase in the wake of the attacks". The authors "hypothesise that attitudinal changes from media coverage act as an underlying driver".[378]

An experimental study involving showing people pictures of the London bombings found that the images made them feel more threatened and experience less emotional well-being; but that the pictures had less such effect when accompanied with text providing "background information about the terrorists' potential economic, historical and social motives". The study authors note that this may be because meaning "provides people with an increased sense of control and security", or alternatively because thinking helps keep (fearful) emotions in check. They conclude that while this was a small and limited experimental study, its policy implications would be that victims may benefit from counselling that involves understanding attackers' motives and that "the frightening effect of terrorist threat can be altered by the way media reports about terrorism".[379]

Media response

Some commentators have noted that, for the UK at least, the 7/7 bombings represented something of a broadcasting sea-change in certain respects. Richard Sambrook, then director of the BBC's World Service and Global News division,

[377] Hussain, Yasmin, and Paul Bagguley, "Funny Looks: British Pakistanis' experiences after 7 July 2005", *Ethnic and Racial Studies*, Vol. 36, No. 1, 2013, pp. 28-46 [pp. 28, 31-36, 39, 39-40].
[378] Hanes, Emma, and Stephen Machin, "Hate Crime in the Wake of Terror Attacks: Evidence from 7/7 and 9/11", Research Paper, November 2012. http://www.sv.uio.no/econ/english/research/news-and-events/events/guest-lectures-seminars/Thursday-seminar/paper/hanes-machin-november-2012.pdf
[379] Fischer, Peter, Tom Postmes, Julia Koeppl, Lianne Conway and Tom Fredriksson, "The Meaning of Collective Terrorist Threat: Understanding the Subjective Causes of Terrorism Reduces Its Negative Psychological Impact", *Journal of Interpersonal Violence*, Vol. 26, Issue 7, pp. 1432-1445, 1434; 1442.

wrote that on the morning of 7 July, BBC News's "initial indication that we were facing more than the 'power surge' the transport authorities were reporting came in an e-mail a viewer sent us". Indeed, "[w]ithin six hours we received more than 1,000 photographs, 20 pieces of amateur video, 4,000 text messages, and 20,000 e-mails". Sambrook casts this as a situation in which "audiences had become involved in telling this story as they never had before", and that public contributions "became an integral part of how the BBC reported the day's events".[380] As Lorenzo-Dus and Bryan note, "[w]hilst this practice [of soliciting user-generated content] is nowadays adopted by almost all television broadcasters…it was virtually unheard of before 7/7".[381]

Allan notes that Manuel Castells has coined the term "mass self-communication" to describe the way that "[t]he diffusion of Internet, mobile communication, digital media, and a variety of tools of social software have prompted the development of horizontal networks of interactive communication that connect local and global in chosen time".[382] These networks "challenge…institutionalised power relations", yet are also "rapidly converging with the mass media". On the day of the bombings, Allan suggests, the phenomenon Castells identifies is useful in understanding "the spontaneous actions of ordinary people compelled to adopt the role of a journalist in order to bear witness to what was happening" that day.[383] Moreover, the way that people consumed news was also different from previous decades, and "[f]or many Londoners, especially those who were deskbound in their workplaces, the principal source of breaking news about the attacks was the Internet". Websites, such as *BBC News* and *The Guardian*, also enabled ordinary users to submit their (in many cases, compelling and dramatic) first-hand accounts of events that morning. In particular, though, it was the fact that many members of the public had "mobile telephones equipped with digital cameras" that generated imagery from places journalists couldn't access themselves, as well as images that captured the ghostly aftermath. [384] On the other hand, it has also been noted that "mobile media files [broadcast] showed very few casualties"[385] – presumably as a result of editorial, cultural and legal reasons in UK broadcasting – but which thus gave only a partial representation of the gruesome events.

In addition to enabling user-generated media to be conveyed to broadcasters and journalists, the Internet has enabled some citizens to create their own websites as a kind of creative "outlet" for peaceful expression of resilience in the face of terrorism, especially in relation to specific terror attacks including the London bombings. The

---

[380] Sambrook, Richard, "Citizen Journalism and the BBC", *Nieman Reports*, Vol. 59, No. 4, Winter 2005, pp. 13-16.
[381] Lorenzo-Dus, Nuria and Annie Bryan, "Recontextualizing participatory journalists' mobile media in British television news: A case study of the live coverage and commemorations of the 2005 London bombings", *Discourse & Communication*, Vol. 5, No. 1, 2011, pp. 23-40, p. 25.
[382] Castells, Manuel, "Communication, power and counter-power in the network society", *International Journal of Communication*, Vol. 1, No. 1, 2007, pp. 238-266, p. 246; cited in Allan, Stuart, "Citizen Journalism and the Rise of "Mass Self-Communication": Reporting the London Bombings, *Global Media Journal: Australian Edition*, Vol. 1, Issue 1, pp. 1-20, p. 2.
[383] Allan, Stuart, "Citizen Journalism and the Rise of "Mass Self-Communication": Reporting the London Bombings, *Global Media Journal: Australian Edition*, Vol. 1, Issue 1, pp. 1-20, [p. 1, 2].
[384] Ibid., pp. 5, 9-10, 12.
[385] Lorenzo-Dus, Nuria, and Annie Bryan, "Recontextualizing participatory journalists' mobile media in British television news: A case study of the live coverage and commemorations of the 2005 London bombings", *Discourse & Communication*, Vol. 5, No. 1, 2011, pp. 23-40 [p. 29].

site, named "We're Not Afraid"[386], contains some aphorisms and affirmations ("We are not afraid to ride public transportation", "We are not afraid to say that terrorism in any form is never the answer" and a self-description of the site as "an outlet for the global community to speak out against the acts of terror… occurring in cities around the world each and every day". The website seems in fact to have been created in particular in response to the London bombings. While the site appears no longer maintained, the greater part of the website remains online, and features photographs and other imagery edited to include slogans such as "We're Not Afraid" and similar, expressing citizens' "resilience".

Hoskins and O'Loughlin have studied a different aspect of reporting of security issues, looking in particular at security reporting since 7 July 2005, arguing that "security journalism" can be considered an important sub-genre of news. Security journalism's delivery of Al-Qaeda speeches is particularly significant, they argue, because it "repackag[es] and remediat[es] jihadist media productions…offer[ing] to British audiences 'messages' presumed to be radicalizing to would-be jihadist recruits". However, their own research, involving interviews and a focus group, all with British Muslims, found that their participants were quite discerning in their media consumption, and that they were somewhat critical of certain aspects of jihadist media productions, regarding them as out of touch with Western Muslims' experiences.[387]

Conclusions from an IRISS perspective

- From the perspective of the Montpellier-derived, IRISS model of stresses, shocks and resilience trajectories, the London bombings event itself appears of sufficient magnitude and significance as to be classed as a "shock" event.
- From a broader and longer-term perspective, however, we can also see various stresses involved, for example, the challenges faced by the intelligence services in dealing with greatly increased case-load regarding potential suspects or the challenges to democratic rights posed by legal and institutional responses.
- In the case of the London bombings and thereafter, we can identify "resilience" as featuring in several different and often countervailing ways – for example, resilience to terrorist attack, resilience to increased surveillance and psychological resilience.
- Resilient responses of various kinds can often usefully be understood as located in a temporal sequence of events, including as responses to previous responses.
- We cannot say that event X *caused* response Y (e.g., that the War in Iraq *caused* the London bombers to carry out their attacks) but we can see how prior events may be important factors in understanding how certain responses came about.
- Neither is this to say in any way that response Y is therefore *morally justified* by event X.
- Some resilient responses may have highly negative and counter-productive consequences.

[386] http://www.werenotafraid.com

[387] Hoskins, Andrew, and Ben O'Loughlin, "Security journalism and 'the mainstream' in Britain since 7/7: translating terror but inciting violence?", *International Affairs*, Vol. 86, No. 4, 2010, pp. 903-924 [pp. 904, 918, 914].

- Resilience measures can often learn well from prior events and aim to mitigate future adverse events. However, currently, resilience measures do not always anticipate very well their sometimes highly negative and counter-productive consequences.

3.2.4 The Mumbai terrorist attacks 2008 ("26/11")

Dr Rowena Rodrigues, Trilateral Research & Consulting

Nature of the adverse event

The 26/11 attacks, as they are commonly known, refer to a series of co-ordinated shooting and bomb attacks by a terrorist group called Lashkar-e-Taiba (LeT) that took place in Mumbai, India, from 26 to 29 November 2008. A total of 166 people were killed and more than 300 wounded. The attacks occurred at a diverse range of locations such as the Chhatrapati Shivaji Terminus (one of the world's busiest train stations), the Oberoi Trident (hotel), the Taj Mahal Palace and Tower (hotel), Leopold Café (a popular restaurant), Cama Hospital (a women and children's hospital), Nariman House (a centre of the Jewish Chabad Lubavich community), Metro Cinema, a lane behind the Times of India building, and St Xavier's College. Explosions occurred at Mazagaon (Mumbai's port area) and in Vile Parle. Only one of the persons involved, Ajmal Kasab, was apprehended.

The attacks proved to be an immense shock, and had an international impact and implications particularly for the USA[388] and Pakistan. Subsequent investigations revealed that the attacks had been pre-planned by Lashkar-e-Taiba (LeT) (who had gathered information and used a US citizen of Pakistani origin David Headley to operationalize the attacks).[389] Pakistan's Inter Service Intelligence (ISI) along with other LeT leaders and commandoes from Pakistan also played a major part in the planning of the attacks.

The impact of the attacks was immense; it affected Indian policy-making at the highest level and all sectors of society at the core, ground level. The occurrence of the attacks across a variety of locations meant that their impact was maximised across sectors and society. Target profiles of victims included citizens and foreign nationals (specifically US and British), travellers, hotel guests, vulnerable individuals such as patients and children, religious minority, students, security forces, etc.

Subsequent investigations revealed that the attacks had been planned in advance. The attackers entered India by sea after hijacking an Indian fishing trawler and murdering its crew. This enabled them to successfully elude security checkpoints and avoid suspicion. The attackers used a variety of tools such as assault rifles, hand grenades, improvised explosive devices, pistols, and a combination of means such armed assaults, barricade and hostage situations, building takeovers, hijackings, drive-by

[388] Kronstadt, K. Alan, *Terrorist Attacks in Mumbai, India, and Implications for U.S. Interests*, Congressional Research Service, Report for Congress, Washington, 19 December 2008.
[389] A US court sentenced David Headley to 35 years in prison for his role in the Mumbai attacks. Tarm, Michael, "American Mumbai plotter sentenced to 35 years", *Washington Times,* 24 January 2013. http://www.washingtontimes.com/news/2013/jan/24/american-mumbai-plotter-sentenced-35-years/

shootings, prefabricated improvised explosive devices (IEDs) and targeted killings (of policemen and selected foreigners).[390] The attacks created pandemonium in the city. A RAND report summarises the gravity of the attack:

> The Mumbai attack reflected precise planning, detailed reconnaissance, and thorough preparation, both physical and mental. It relied on surprise, creating confusion and overwhelming the ability of the authorities to respond. And it required determined execution by suicide attackers who nonetheless were able to operate effectively over an extended period of time.[391]

Institutional response

Despite having some intelligence that the LeT might infiltrate India through a sea route in 2008, Indian central intelligence agencies had issued no such specific alert.[392] However, based on an alert dated 9 August 2008 of a bomb attack at various places, the District Commissioner of Police (DCP) (Zone 1) along with his staff visited the threatened areas and had issued written security instructions.[393] The police warned the Oberoi Trident hotel and conducted security briefings for representatives of other hotels, malls, multiplexes on 12 August 2008. After the receipt of an Intelligence Bureau alert dated 24 September 2008 that LeT was showing an 'interest' in Taj Mahal Palace Hotel and other sites, another meeting was held with Taj security personnel on 29 September 2008 by DCP Zone-1 and a subsequent security briefing was held at the hotel. Similar actions were also taken in relation to Café Léopold and the police reportedly sensitised the restaurant owner about the threat.

The simultaneous nature of the attacks created panic in the city of Mumbai and overwhelmed the security forces. The police control room systems were overloaded and personal devices had to be used for communication. Police units were deployed in "a haphazard and helter-skelter manner".[394] The attackers used their strategic positioning to attack the police and security forces. Some of the police despite being only equipped for normal policing duties (with sticks, gas guns and some even without bullet proof vests) showed great bravery in dealing with the attackers.

The police and security forces (Army, Navy and National Security Guard) launched operations (e.g. Operation Tornado) against the attackers in the two hotels and at Nariman House, a Jewish residential complex. The Times of India reports that the forces rescued 250 people in Oberoi, 300 in Taj and 12 families of 60 people in Nariman House and recovered two AK-47 rifles, nine magazines, two pistols and mobile phones from Nariman House, while in Trident Oberoi two more AK-47 rifles, eight magazines and two pistols were seized.[395]

---

[390] Rabasa, Angel et al., "The Lessons of Mumbai", *Rand Occasional Paper*, 2009. http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf
[391] Ibid.
[392] Pradhan, Ram D., V. Balachandran, *Report of the High Level Enquiry Committee (HLEC) on 26/11,* 18 April 2009. http://maharashtratimes.indiatimes.com/photo.cms?msid=5289960
[393] Pradhan and Balachandran, op. cit, 2009.
[394] Pradhan and Balachandran, op. cit, 2009
[395] Agencies, "Battle for Mumbai ends", *Times of India,* 29 Nov. 2008. http://articles.timesofindia.indiatimes.com/2008-11-29/india/27930171_1_taj-hotel-three-terrorists-nariman-house

After the event, the State of Maharashtra set up a high-level committee comprising former home secretary Ram D. Pradhan and former Indian Police Service officer V. Balachandran to "analyse how far the existing procedures, instruments and administrative culture are to be blamed for what are perceived as lapses".[396] The committee sought to identify systemic failures and recommend steps to mitigate future attacks.[397]

The report found that the administration and enforcement agencies had been generally unprepared for the attack. While it did not find "any serious lapses in the conduct of any individual officer", it found a lack of: intelligent appreciation of threats; handling of intelligence;[398] efficiency in instruments specifically set up to deal with terrorist attacks; overt and visible leadership in facing multi-targeted attacks; sensitisation of officers to new threats. The Committee made 25 recommendations and proposed a standard operating procedure to deal with terrorist attacks. The Committee recommended: that the police should attempt to function cooperatively; that no officials should be able to override structural command and control systems to suit individual predilections; that special forces set up to deal with such events must be used effectively; further investment in recruitment and training of personnel, and the need for improved equipment and means to deal with such attacks. In addition, the Committee suggested the Mumbai police be permitted access to CCTV cameras installed in private premises such as hotels, training of private sector security personnel in handling such devices, underlined a need for a "closer liaison between the Mumbai city police and mobile service providers" to detect terrorist links, and recommended upgrading the Mumbai police's cellular monitoring capabilities. However, many of the Committee's recommendations were not implemented.[399]

As one writer suggests, the event "exposed India's inadequate resources for counter-terrorism and highlighted the failure to anticipate and robustly respond to major incidents".[400] To make his point, the writer cites the ineffective responses of the first responders to the attacks and the use of "antiquated bolt action rifles" by the Railway Protection Force (RPF) at CST Terminus against the attackers advanced weapons. Others have criticised the National Security Guard (NSG) for its late and ineffective response.[401] One article suggests that the shortcomings in India's urban police forces "ensured that the attackers were neither challenged on landing nor neutralized at the Chhatrapati Shivaji Terminus before wreaking havoc on a population".[402] The author highlights the inadequacies of equipment, unarmed nature of civil police, poor

---

[396] Appointed by the Maharashtra Government vide GAD GR No: Raasua.2008/C.R.34/29-A, 30 Dec. 2008.

[397] Pradhan and Balachandran, op. cit, 2009

[398] Pradhan and Balachandran, op. cit, 2009. The Pradhan Committee found "total confusion in the processing of intelligence alerts at the level of State Government".

[399] Marpakwar, Prafulla, "Mumbai Blasts: Govt. Fails to Keep its Word", *Times of India,* 15 July 2011. http://articles.timesofindia.indiatimes.com/2011-07-15/mumbai/29777553_1_terror-attacks-coastal-areas-ips-officer

[400] Patel, Avnish, "After Mumbai- India's response," RUSI Analysis, Commentary, 25 Nov 2009. http://www.rusi.org/analysis/commentary/ref:C4B0D3DCA5D253/#.UefGuN9wbrc

[401] Rabasa, Angel et al, "The Lessons of Mumbai", *Rand Occasional Paper*, 2009. http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf. Subsequent to the attacks, the NSG set up regional centres to enable it to respond better to future crises.

[402] Badri-Maharaj, Sanjay, "The Mumbai Attacks - Lessons to be Learnt from the Police Response", *Journal of Defence Studies*, Vol. 3, No. 2, 2009, pp.145-156.

response time, poor communications, leadership and co-ordination as key factors that contributed to maximising the impact of the attacks.[403]

The event had a political fallout and resulted in the resignations of Union Home Minister, Shivraj Patil (responsible for national security), the Chief Minister of Maharashtra Vilasrao Deshmukh and the Deputy Chief Minister R.R. Patil (who made some insensitive comments about the event that resulted in a public reaction). The event thus had some impact on political accountability.

The coastal monitoring failure prompted the government to revisit coastal security measures. Several measures such as coastal surveillance sensors, biometric identity cards for fishermen were proposed. In 2009, the Department of Animal Husbandry, Dairying and Fisheries (Ministry of Agriculture) launched a central scheme called 'Issuance of Biometric Identity Cards to Coastal Fishermen'.[404] One of the scheme's main objectives was to "strengthen Coastal security and the threat from sea route would be reduced through this mechanism".[405] The Scheme also envisaged the establishment of a National Marine Fishers Database (NMFD) that would be accessible to all Central and State authorised agencies.

In August 2012, the Defence Minister inaugurated the Maharashtra cluster of the chain of static coastal surveillance sensors aimed at providing real-time surveillance along the coastline.[406] The network comprises static radar and electro-optic sensors at 84 remote sites along the coastline and island territories, to detect movement of suspicious vessels. High end surveillance gadgets such as frequency diversity radar, electro-optic sensor, video high frequency (VHF) sets and metrological equipment installed on existing light houses or masts erected at each site will support the system. The Coast Guard regional headquarters will manage the data generated by the static sensors and it will be coordinated with the Vessel Traffic Management Systems of the major ports and the fishing vessel monitoring system.

The most significant response was the passing of the National Investigation Agency Act, 2008 which laid the foundation for the establishment of the National Investigation Agency (NIA) (currently India's central counter terrorism law enforcement agency)[407] to "investigate and prosecute offences affecting the sovereignty, security and integrity of India, security of State, friendly relations with foreign States and offences under Acts enacted to implement international treaties, agreements, conventions and resolutions of the United Nations".[408] The NIA's activities include: in-depth professional and scientific investigation of scheduled offences, ensuring effective and speedy trials, maintaining professional and cordial

---

[403] Ibid.

[404] Department of Animal Husbandry, Dairying and Fisheries (Ministry of Agriculture), "Issuance of Biometric Identity Cards to Coastal Fishermen". http://www.dahd.nic.in/dahd/division/fisheries/issuance-of-biometric-identity-cards-to-coastal-fisherman.aspx

[405] Ibid.

[406] Press Information Bureau, "Defence Minister AK Anthony inaugurates Maharashtra Cluster of Coastal Surveillance System," 25 August 2012. http://pibmumbai.gov.in/scripts/detail.asp?releaseId=E2012PR3797

[407] NIA. http://nia.gov.in/

[408] The National Investigation Agency Act, Act No. 34 of 2008. http://www.nia.gov.in/acts/The_National_Investigation_Agency_Act_2008.pdf

relations with the governments of States and Union Territories and other law enforcement agencies in compliance of the legal provisions of the NIA Act, assisting the states and other investigating agencies in investigation of terrorist cases, building a terrorist information database and sharing information with the states, studying and analysing laws relating to terrorism in other countries and regularly evaluating the adequacy of existing laws in India and propose changes when required. Despite its positive elements, the Agency has been criticised for being a "reactive rather than proactive entity".[409]

Judicial response

A Mumbai trial court sentenced Ajmal Kasab to death on all 86 charges[410] of his conviction. The Bombay High Court and the Supreme Court of India rejected his appeals and upheld his death sentence.[411] Only the *rarest of the rare* cases in India merit the death sentence.[412] The Supreme Court in upholding the death sentence commented that Kasab's case fulfilled all the established criteria in which death sentences are awarded:

- when the murder is committed in an extremely brutal, grotesque, diabolical, revolting or dastardly manner so as to arouse intense and extreme indignation of the community;
- when the murder is committed for a motive which evinces total depravity and meanness;
- when murder of a member of a Scheduled Caste or minority community, etc., is committed not for personal reasons but in circumstances which arouse social wrath;
- When the crime is enormous in proportion;
- When the victim of murder is (a) an innocent child who could not have or has not provided even an excuse, much less a provocation, for murder (b) a helpless woman or a person rendered helpless by old age or infirmity (c) when the victim is a person whom the murderer is in a position of domination or trust (d) when the victim is a public figure generally loved and respected by the community for the services rendered by him and the murder is committed for political or similar reasons other than personal reasons.

In addition to these, the Supreme Court found other factors that justified the award of the death sentence. For instance, a complex level of cross-border conspiracy to wage war against the Government of India and weaken the country; meticulous planning and preparation for the attacks; high number of fatalities (166) and injured people; colossal loss of property; and Kasab's lack of remorse and repentance. In its judgment, the Supreme Court complimented the "resilient spirit of Mumbai that, to all

---

[409] Patel, Avnish, "After Mumbai- India's Response", RUSI Analysis, 25 Nov. 2009. http://www.rusi.org/analysis/commentary/ref:C4B0D3DCA5D253/#.Ue5gw99wbrc

[410] The key charges included: conspiracy to wage war against the Government of India; collecting arms with the intention of waging war against the Government of India; waging and abetting the waging of war against the Government of India; commission of terrorist acts; criminal conspiracy to commit murder; criminal conspiracy, common intention and abetment to commit murder; committing murder of a number of persons; attempt to murder with common intention; criminal conspiracy and abetment; abduction for murder; robbery/dacoity with an attempt to cause death or grievous hurt; and causing explosions punishable under the Explosive Substance Act, 1908.

[411] *Md. Ajmal Md. Amir Kasab v State of Maharashtra*, Supreme Court, 29 August 2012. http://indiankanoon.org/doc/78874723/

[412] *Machhi Singh v State of Punjab* (1983) 3 SCC 470

outward appearances, recovered from the blow very quickly and was back to business as usual in no time".[413] After the President of India rejected his mercy petition, Kasab was hanged to death in secret at Yerawada jail in Pune on 21 November 2012.

Societal response

The media's response to the attacks was two-fold: to function as means of communication and dissemination, and to carry out institutional review and oversight. The mass media (national and international) played a crucial role in providing information during and after the Mumbai attacks. They also monitored institutional actions during and post-Mumbai. They highlighted the institutional failures[414] such as that of the police and security forces in dealing with the attacks.[415]

However, the media distorted the value of its good work by engaging in some sensationalism and irresponsible coverage of the attacks. The criticisms were sharp – some critics specifically questioned the manner in which the media over-sensationalised the attacks. Other critics highlighted the "TV terror" unleashed by the 24-hour television news channels in their coverage of the event.[416] The concerns related to the broadcasting of gruesome scenes of the attacks, aggressive handling of the event and inaccurate reporting. Some representatives of the media themselves admitted their failure, stating "we did well getting into the line of fire, but from an ethical point of view we screwed up big-time."[417] The 26/11 coverage had such an impact that a News Broadcasters Association (NBA),[418] representing private television news and current affairs broadcasters, was formed in 2008 and the News Broadcasting Standards (Disputes Redressal) Authority was established to enforce the NBA's Code of Ethics & Broadcasting Standards,[419] which became operational from 2 October 2008.

The academic response to the Mumbai attacks was varied. The community responded by highlighting the deficiencies in the Indian security and policing.[420] A large number

---

[413] *Md. Ajmal Md. Amir Kasab v State of Maharashtra*, Supreme Court, 29 August 2012. http://indiankanoon.org/doc/78874723/

[414] Swami, Praveen, "Mumbai attacks: One year on", *BBC News,* 25 November 2009. http://news.bbc.co.uk/1/hi/world/south_asia/8373836.stm

[415] For instance, Swami, Praveen, "Desperate Need for National Police Tactics and Weapons School", *The Hindu*, 11 December 2008.

[416] Pepper, Daniel, "India's media blasted for sensational Mumbai coverage", *Christian Science Monitor,* 24 Dec. 2008. http://www.csmonitor.com/World/Asia-South-Central/2008/1224/p01s01-wosc.html

[417] Ibid. Statement by Shishir Joshi, the editorial director of Mid-Day, a Mumbai newspaper.

[418] The NBA has 47 members. http://www.nbanewdelhi.com/

[419] See News Broadcasting Standards Regulations. http://www.nbanewdelhi.com/newsbroadcasting-standards-dr-regulations.asp

[420] Raman, B., *Mumbai 26/11: A Day of Infamy,* Lancer Publishers, New Delhi, 2009. Shankar, D., M. Agrawal and H.R. Rao, "Emergency Response to Mumbai Terror Attacks: An Activity Theory Analysis" in R. Santanam, M. Sethumadhavan and M. Virendra (eds.), *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives*, 2011, pp. 46-58; Badri-Maharaj, Sanjay, "The Mumbai Attacks - Lessons to be Learnt from the Police Response", J*ournal of Defence Studies*, Vol. 3, Issue 2, 2009, pp. 145-156. Foreman, Jonathan, "India's Time of Reckoning", *Commentary,* Feb. 2009, pp. 20-24. http://www.commentarymagazine.com/article/india%e2%80%99s-time-of-reckoning/

of academic papers called for improvement in India's counter-terrorism policy.[421] Others called for a developing a strategic security framework. Some papers document the growth of citizen journalism,[422] "ambient journalism"[423] or distributed surveillance.[424] Some highlighted the rise of "new terror architecture". [425] Some papers focussed on the organisational aspects of the attackers (or groups orchestrating the attacks),[426] others analysed the links between the attacks and technology.[427] One paper documented and analysed victim-related issues such as stress disorders.[428] Another academic paper[429] researching the Mumbai attacks calls for greater use of social networking analysis (SNA) by security agencies and tries to justify that SNA "can be a powerful tool for understanding the complex nature of terrorist organisations", even if only limited information is available from open sources. It suggests that "identification of type of terror networks would provide useful inputs to strengthen counter-terrorism efforts" despite recognising that "SNA alone would not suffice for unravelling the modus operandi of terrorist networks".[430] All this has contributed to a deep, varied and rich, study and policy resource on such attacks and responses to them.

The actions of individuals took centre stage during and after the Mumbai attacks. Individuals, in different capacities (either as employees,[431] members of the police or security forces or as citizens) acted in a number of ways that helped to reduce or mitigate the effects of the Mumbai attacks. These actions were documented live during the attacks and have even become case studies for business and crisis management. For example, 'Terror at the Taj Bombay: Customer-Centric Leadership'

---

[421] Staniland, Paul, "Improving India's Counterterrorism Policy after Mumbai", *CTC Sentinel*, Vol. 2, Iss. 4, 2009, pp.11-14.

[422] Bahador, Babak, and Serene Tng, "The Changing Role of the Citizen in Conflict Reporting", *Pacific Journalism Review*, Vol. 16, Issue 2, 2010, pp.178-194 [p. 178].

[423] Hermida, Alfred, "Twittering the News: The Emergence of Ambient Journalism", *Journalism Practice*, Vol. 4, Issue 3, 2010, pp. 297-308.

[424] Heverin, Thomas, "Microblogging for distributed surveillance in response to violent crises: Ethical considerations", *Proceedings of the 2011 iConference* (iConference '11), ACM, New York, 2011, pp. 827-828.

[425] Rath, Saroj Kumar, "New Terror Architecture in South Asia 26/11 Mumbai Attacks Inquiry", *India Quarterly: A Journal of International Affairs,* Vol. 66, Issue 4, 2010, pp. 359-381.

[426] Acharya, Arabinda, and Sonal Marwah, "Nizam, la Tanzim (System, not Organization): Do Organizations Matter in Terrorism Today? A Study of the November 2008 Mumbai Attacks", *Studies in Conflict & Terrorism*, Vol. 34, Issue 1, 2010, pp. 1-16. Tankel, Stephen, "Lashkar-e-taiba: From 9/11 to Mumbai", in Harvey Rubin (ed.), *Developments in Radicalisation and Political Violence*, University of Pennsylvania, Philadelphia, 2009.

[427] LaRaia, William, and Michael C. Walker, "The siege in Mumbai: A conventional terrorist attack aided by modern technology" in M. R. Haberfeld and Agostino Hassell (eds.), *A New Understanding of Terrorism: Case Studies, Trajectories and Lessons Learned,* Springer, New York, 2009, pp. 309-340.

[428] Balasinorwala, Vanshree Patil, and Nilesh Shah, "Acute stress disorder in victims after terror attacks in Mumbai, India", *The British Journal of Psychiatry,* Vol. 195, Issue 5, 2009, pp. 462-462.

[429] Azad, Sarita and Arvind Gupta, "A Quantitative Assessment on 26/11 Mumbai Attack using Social Network Analysis", *Journal of Terrorism Research*, Vol. 2, Issue 2, pp. 4-14. Dr Sarita Azad is a researcher at Institute for Defence Studies and Analyses, New Delhi, India. Dr. Arvind Gupta holds the Lal Bahadur Shastri Chair at the Institute for Defence Studies and Analyses, New Delhi, India (and leads the Internal Security Cluster).

[430] Ibid.

[431] See also Paul, Rik, "Taj: I will prevail. Exemplifying customer service in times of crisis", *Emerald Emerging Markets Case Studies Collection*, (2012). http://www.emeraldinsight.com/case_studies.htm?articleid=17076737

is a multimedia case study in the Harvard Business School – it "documents the bravery and resourcefulness shown by rank-and-file employees during the siege".[432]

During the event, individuals acted proactively, supported institutional actors and filled gaps in institutional actions. For instance, some individuals witnessing the attacks used their mobile phones and other devices to record events and disseminate information (written and pictorial, some of which raised ethical questions) through social media such as Facebook and Twitter.[433] Twitter, for instance, was used both to disseminate news and provide eyewitness accounts of the attacks.[434] Other individuals (such as the Taj hotel employees) went beyond the requirements of their job to mobilise and help victims during the attack; some died as a result.[435]

One key public reaction was anger and resentment at being left vulnerable and the institutional lack of ability to prepare for and defend against such an attack.

Vir Sanghvi (and Indian print and television journalist, columnist, and talk show host) characterises the Indian response to the Mumbai attacks as "unique".[436] He states, "Indians are used to terrorism. It no longer shocks us as it once did. Nor are we startled by the recognition that Pakistan might be involved. We have come to accept this as a part of our lives."[437] He further suggests that people in places such as Mumbai are aware of their vulnerability and underlines how there were no "knee-jerk responses" to the event or attempts to "make scapegoats of Indian Muslims."[438]

Economic response

The 26/11 attacks specifically impacted two well-known international brands – the Taj and Oberoi. One research paper specifically analyses the case of the Taj Hotel (flagship hotel of the Taj Hotels Resorts and Palaces and a part of the Tata Group) and shows how the company successfully responded to the impact of the attacks.[439] Without talking about resilience itself, the author presents a case of how the Taj equipped itself before and responded during the attack, which helped it bounce back from the impact of the attack. Before the attacks occurred, the Taj had a number of preventative measures in place (such as security scanners, CCTV, sniffer dogs).

---

[432] Hanna, Julia, "Terror at the Taj Bombay: Customer-Centric Leadership", Harvard Business School, 24 Jan. 2011. http://hbswk.hbs.edu/item/6602.html

[433] Stelter, Brian and Noam Cohen, "Citizen Journalists Provided Glimpses of Mumbai Attacks" *The New York Times,* 30 November 2008. Beaumont, C. "Mumbai attacks: Twitter and Flickr used to break news", *The Daily Telegraph*, 27 Nov. 2008. Dolnick, Sam, "Bloggers provide raw view of Mumbai attacks", *MSNBC*, 30 Nov. 2008. http://www.msnbc.msn.com/id/27984057/ns/technology_and_science-tech_and_gadgets/

[434] Murthy, Dhiraj, "Twitter: Microphone for the masses?" *Media, Culture and Society,* Vol. 33, Iss. 5, 2011, pp. 779-789.

[435] Indo-Asian News Service, "Special tourism awards for Taj, Oberoi," *MSN Lifestyle,* 25 Feb. 2009. http://lifestyle.in.msn.com/travel/article.aspx?cp-documentid=3191288

[436] Sanghvi, Vir, "Introduction", in Hindustan Times (ed.), *26/11: The Attack on Mumbai,* Penguin Books India, 2009.

[437] Ibid.

[438] Sanghvi, Vir, "Introduction", in Hindustan Times (ed.), *26/11: The Attack on Mumbai,* Penguin Books India, 2009.

[439] Balakrishnan, Melodena Stephens, "Protecting from brand burn during times of crisis: Mumbai 26/11: A case of the Taj Mahal Palace and Tower Hotel", *Management Research Review*, Vol. 34, Issue 12, 2011, pp.1309 -1334.

During the crisis stage, Taj took several measures: set up a war room, kept the community informed through a microsite and used senior managers to minimise collateral damage. During this stage the author suggests that the Taj "was proactive in keeping the information flowing, enhancing their reputational reservoir despite being constrained by some external stakeholders' lack of preparedness".[440] Taj also focussed on positive elements (such as the grand history of the Taj and Tata's and India's unity). During the post-crisis stage, the author highlights how the Taj took a proactive and "unified stance in communication", making use of employee welfare tools and providing them with psychological support. Finally, the author concludes that the Taj succeeded in minimising brand burn by "using proactive actions and information management focused on building a reputational reservoir, finding an older, empathetic endorser brand in the brand architecture to lean on, reframing from functional to symbolic components, actively engineering word of mouth (WOM) and keeping a common message".[441]

Both the Taj and the Oberoi Trident reopened after the attacks with minimal economic fallout. A year after the attacks, even the Leopald Café was doing brisk business.[442]

Despite gloomy headlines,[443] many industry players downplayed the attacks and highlighted the resilient nature of Mumbai.[444] One report even goes so far as to suggest that following "Nathan Rothschild's maxim that the best time to buy shares is when blood runs in the streets", foreign investors "bought $151 million worth of Indian stocks and bonds on 28 November 2008 in the middle of the Mumbai gunfight, and invested $524 million into India's equity and debt markets during the first 12 days of December 2008.[445] To a large extent, this shows that Mumbai's industry and the Indian economy has, over the years, built some form of resilience to terrorist attacks and this was evident during and after the attacks.

Critical conclusions from an IRISS perspective

A non-robust, non-dynamic, uncoordinated and conservative institutional setup that does not learn from global and local adverse events) can lead to a failure in dealing with multi-actor, multi-modal terrorist attacks. Such a set up fundamentally weakens the country or society that relies upon it and leaves it vulnerable to new and evolving forms of threats. Therefore, it is essential that institutions invest in the right resources (human and technological) to deal with such threats; following up of the effective use of such resources is also crucial. There must be adequate follow-up to ensure that

[440] Balakrishnan, op. cit., 2011

[441] Balakrishnan, op. cit., 2011.

[442] Irani, Delnaaz, "Business as usual a year after Mumbai attacks", *BBC News*, 26 November 2009.

[443] Zachariah, Reeba, "Attacks may have cost Rs 50k cr", *Times of India*, 1 December 2008. http://articles.timesofindia.indiatimes.com/2008-12-01/india-business/27949750_1_tax-collections-taj-and-oberoi-single-screen-theatres

[444] Ibid. For instance, Bundeep Singh Rangar stated, "Mumbai is a very resilient city. Each time it's been the target of a terrorist attack, it rebounds stronger and more resolute." Zachariah, Reeba, "Attacks may have cost Rs 50k cr", *Times of India*, 1 Dec 2008. http://articles.timesofindia.indiatimes.com/2008-12-01/india-business/27949750_1_tax-collections-taj-and-oberoi-single-screen-theatres

[445] Aiyar, Swaminathan S. Anklesaria, "Investors swoop in after Mumbai attacks", Commentary, *Forbes,* 2 Jan. 2009.

learning from adverse events can actually help contribute to a safer and more resilient society.

Societal actors, particularly individuals, are key factors in resilience building. A society with resilient individuals who have the propensity and capacity to collaboratively meet adversity contribute to a stronger society and country, ensuring that an adverse event only has a greater shorter term impact rather than an invidious, longer term impact.

3.2.5 The Boston bombing

Dr Reinhard Kreissl, Institute for the Sociology of Law and Criminology (IRKS)

Nature of the adverse event

On 15 April 2013 at 2:49 pm EDT, an explosion hit the Boston marathon near the finish line at Boylston Street. Two bombs exploded only seconds apart close to the finish line, killing three people and injuring 264 others. The event known as the Boston Bombing triggered a wide and immediate coverage by different media online and offline around the world in real time and in parallel.

Different stories and interpretations emerged and spread through the web of communication channels. A large number of actors, officials, politicians, law enforcement agents, journalists, and self-proclaimed experts, spontaneous communities built around electronic communication platforms contributed to a debate about the events, sharing information, producing more or less reliable accounts of what had happened and why. This tsunami-like wave of (mainly electronic) communication immediately after the bombing proved to be a stress test not only for the cell-phone infrastructure of downtown Boston. Communication did not break down, but there were reports that cell-phone service locally was temporarily shut down to prevent the use of mobile phones as remote detonators.

Institutional response

On the ground, first responders attempted to handle the damages and injuries. Emergency procedures by police and rescue workers unfolded, providing medical services to the injured and closing the site of the bombings to the public. Nearby buildings were evacuated and forensic teams started to work on the crime scene. Red Cross and emergency services provided help lines for friends and relatives to inform about injured persons.

Emergency measures stretched across the city and the whole Boston area. They were based on the plans developed by Massachusetts Emergency Management Agency (MEMA) who were directly involved in responding to the Boston attacks. The reaction followed a procedure laid down in the “Comprehensive Emergency Plans” and involved organisations at the local, state and federal level. The coordination of these different actors is the task of the Incident Command System and the National Interagency Management System. As an immediate reaction to the events, Logan International Airport was closed, as was public transport in Boston. At a number of

other locations, bomb alarm was triggered but as it turned out, no other explosive devices were planted in the city.

The forensic teams working the crime scene found evidence for the type of explosives used in the attack. As it turned out, the bombs were made using pressure cookers and they were transported in backpacks. But initially no suspects were identified. Due to the wide use of smart phones by the public and the footage of CCTV cameras in the area, a large number of images were available for the authorities documenting the crime scene before the bombs exploded. Despite this comprehensive visual database, no suspects could be identified for the next two days. Nonetheless, an uncontrolled manhunt started on social media platforms, based on media reports, stories and images circulated on these platforms. To curb the dynamic of this rather explosive situation, the police released images of two alleged suspects taken by a security camera close to the bomb scene. Releasing these photos did not lead to an identification or arrest of the two individuals who had planted the bomb.

It was only after a subsequent event at the nearby MIT campus, where the two offenders were involved in a fatal shooting with a police officer after carjacking a vehicle that police could close in on them. They had driven to MIT campus with a car registered under their father's name and DMV records enabled their identification. What followed was a two-day hunt where one of the two suspects was shot by the police in a hold-up and the other was captured by police officers while hiding in the backyard of a private home underneath a boat cover.

The resources mobilised by different law enforcement agencies while searching for the two suspects demonstrated the level of technical hardware built up after 9/11, for the first time fully deployed in a real-world situation. According to media reports during the shoot-out where one of the two suspects was wounded and/or killed by the police within a 10-minute span, "police officers fired what may be an unprecedented number of rounds in a single police incident in recent state history ... [spraying] the neighborhood ... [leaving] at least a dozen nearby houses pockmarked with dozens of bullet holes".[446]

After both suspects were identified as Tsarnaev brothers and the surviving younger brother was arrested, it turned out that different law enforcement agencies had collected information about their prior history, qualifying both as potential radical Islamic activists. The intelligence was available and distributed across different agencies, from Boston police to the Federal Bureau of Investigation (FBI). Russian Intelligence Services had informed US authorities two years before the event about the radical religious affiliation of the two suspects.

The role of surveillance in this adverse event

Surveillance cameras were in place across the area of the event in downtown Boston. Intelligence was available on the two culprits prior to the attacks. Video footage and photographic images from private citizens were made available via social media

[446] Murphy, Sean P., and Todd Wallack, "Witnesses suggest friendly fire felled MBTA officer", *The Boston Globe*, 7 May 2013. http://www.bostonglobe.com/metro/2013/05/06/bullet-that-nearly-killed-mbta-police-officer-watertown-gunfight-appears-have-been-friendly-fire/kIv9CYo0oVGBC3DlhFjelL/story.html

platforms and were collected by law enforcement agencies (LEA). This information did not prevent the bombings or alert the LEA in advance. A threat assessment made prior to the event did not show any extremely high level of danger.

CCTV footage was used to inform the public about the alleged suspects. It should be kept in mind though that Boston police released their images at an early stage primarily to curb the emerging vigilant manhunt developing on social media platforms.

Looking at the supply of information, we see an overload of visual images and intelligence data. This demonstrates a number of more general points: the problem is with data-analysis and not with data gathering; controlling the use of data can be a problem. Rumours spreading uncontrolled through the social media can create a dangerous situation of vigilantism that might affect innocent persons.

At the level of court proceedings, the available images and video footage have to be considered as evidence to be introduced into the hearing by attorneys and prosecutors. It is still not clear how this massive amount of information can be systematically introduced into the courtroom proceeding, how it will be assessed and evaluated by the court. A number of intricate legal issues (e.g. admissibility) have to be solved when it comes to the use of this information.

Resilience in the reaction to this event

Citizens present on the scene after a brief reaction of panic and shock seemed to react adequately, providing help and supporting the rescue workers. The public also provided available evidence (pictures from private smart phones, etc.) to the authorities.

At the same time, the news spread at speed of light through different channels nationwide, triggering a number of pre-emptive reactions across the country. Police and security forces were put on alert, air-traffic in the Greater Boston area was affected, as was public transport. Planes were kept on the ground; buses and trains came to a halt. A large area of several blocks was closed and declared to be a crime scene. Security forces reacted swiftly, though critical observers talked about massive over-reaction, high-tech equipment was deployed, the National Guard and special squads, established after 9/11, were called in to support local forces in the arrest of the suspect.

Media response

At the national level, news coverage was comprehensive and commentators speculated about international terrorist affiliations of the two suspects for days after the event. There were rumours about alleged suspects circulating through public media. The most infamous reaction was the publication on 18 April 2013 of a picture of two men on the front-page of the *New York Post*, who were declared as being suspects for the bombings. The story was taken up by national networks and distributed across the country. A number of innocent individuals also came under suspicion through miscommunications and false allegations spreading through cyber space.

When the surviving offender was finally arrested, Boston staged a party-like celebration, in what could be seen as a reaction of relief. The President gave a speech addressing the nation and promising "to get to the bottom of this". After the bombings, initiatives started to collect money via crowd funding for the victims of the blast; $2 million were donated within a few days through these platforms. For a couple of weeks, a number of sports and cultural events were cancelled following the bombings. Several symbolic events were staged across the country and internationally to honour the victims in the subsequent weeks and months.

Compared to societies that have experienced serious terrorist attacks more frequently, the overall reaction to the Boston bombing seemed a bit exaggerated and overly cautious. As one critic in the Israeli newspaper Haaretz stated, "In terms of cost-benefit analysis, from the evil terrorist's point of view, the Boston Street bombings and their aftermath can only be viewed as a resounding triumph", since the "relatively amateurish" terrorists managed to intimidate a vast number of people and got a maximum amount of publicity.[447] Nonetheless, American society returned to normal after a couple of weeks if not days, focussing attention on other events and newsworthy headlines of national relevance.

Despite a highly dramatic and dramatised public debate and a temporarily explosive situation among self-declared crime fighters from the public, the overall reaction displayed a high level of robustness in the face of the attacks. After an initial arousal, controversial debates about issues such as migration (the two offenders both had migrated with their family from the Caucasus region) persisted for some time but soon faded and disappeared from the headlines.

Conclusions of relevance for IRISS

The Boston bombing clearly qualifies as a major adverse event, disrupting the routine course of social life. With regard to the immediate reaction of the emergency services we find a high level of competence and preparedness. First responders were on the spot and law enforcement personnel acted highly professionally. The public's reaction for some time seemed out of control due to an overload of unstructured information circulating through the social networks. This situation resembled the arrangement, Bauman and Girard describe of explosive communities that search for a scapegoat to be "sacrificed" to restore the attacked order.[448]

The events and the performance of law enforcement clearly demonstrated that surveillance measures were of minor relevance. The offenders were arrested based on evidence provided by standard databases (e.g. DMV files) and citizens' reports. It was good old-fashioned police work and "Inspector Luck" that led to arrests.

In the weeks that followed the event, public debate about increased surveillance clearly produced a balanced view. Arguments in favour of expansion of surveillance were balanced with counter positions pointing to the irrelevance and ineffectiveness of surveillance measures in the context of the event. Boston demonstrated resilience,

[447] Wikipedia, "Boston Marathon Bombings". http://en.wikipedia.org/wiki/Boston_bombing#cite_note-The_Boston_Globe-95
[448] Bauman, Zygmunt, *Liquid Modernity*, Polity Press, Cambridge, 2000.

even though, as observers from other countries with more frequent attacks of this type pointed out, some of the immediate reactions seemed somewhat overblown.

3.2.6 School shootings in Germany

Nils Zurawski, University of Hamburg

It is not fully resolved whether an adverse event has to be a single appearance or whether it could be a series of events that are connected and generate an inner dynamic. This section defines an adverse event rather narrowly. This is not to say that various similar events cannot be analysed as a whole. However, other adversities, that are the consequence of whole strategies that may be disassembled into a series of events that could be defined as adverse, are not in focus here. One example may be the issue of land grabbing in the global south for the food security in the global north. In general, this is adverse politics, but it does not fit into the definition of an event with a genuine impact on its own.

The focus on adverse events directed against citizens and/or the state avoids the perspective on the state as the originator of adverse events, i.e., as in the Israel/Palestine conflict (i.e., both sides); or in cases of authoritarian regimes, how these attack their populations. Lastly, adverse events may also be generated by corporations, as illustrated by the BP case in the Gulf of Mexico or various other hazards around the world. The adversity therein not only lies in the fact of the catastrophe itself, but also in the way the corporations and the states deal with it.

School shootings qualify very well as adverse events. They constitute an attack against humans, albeit very restricted locally. But they always evoke wide and far-reaching discussion on security, its causes, means of protection from potential future occurrences and the use and role of weapons in society as such. All of these aspects and discourses vary depending on the cultural context, the laws and perceptions. This section reports from a German perspective, which holds some similarities with other events in other countries, but does not claim to be a 'fit for all' analyses.

A school shooting is a peculiar event to analyse. Its form and mode of impact and the following shock resemble in many ways a terrorist attack: it is sudden, symbolic, a form of communication and can happen almost anywhere – i.e., at any school. Unlike a terrorist attack, however, a school shooting is most often executed by someone who knows his victims; it is personal, which is generally not a defining feature of a terrorist attack. The perpetrator often frequents such a place e.g., his (rarely her) school and acts out of personal motives, such as hate or revenge. Terrorists generally have a collective ideology or idea behind their actions, while a killing spree in a school is very often, if not always, caused by a deep personal crisis.

The consequences, the impact and shock of school shootings, however, are comparable to that of terrorist attacks. A school shooting might even claim more victims and yet not threaten the state security in comparison to a terrorist attack on representatives of the state or on its citizens. Anders Behring Breivik, the Norwegian who killed 77 people on a small island in Norway on 22 July 2011, was classed a terrorist, while in Newtown, Connecticut, the 20 people killed there were the victims of a school shooting. It is important to note that the conclusions drawn from either a

school shooting or a terrorist attack are totally different. Thus, it is important to take a closer look at an event that has horrific consequences, but that may not affect society as a whole in the same way as another event. School shootings seem to be so shocking, not because of the numbers killed, nor because it is threatening the state or society as such, but because it happens in schools and carried out by pupils (thus far exclusively young men). Schools are seen as safe places, a sheltered environment, where teachers and management try to do everything to protect children. School shootings are inexplicable, not least because they are performed by perpetrators known to their teachers and other pupils. This may intensify the horror and the incomprehension surrounding this event.

This section does not go into the psychology of the perpetrators, or explain the causes of the individual cases. Instead, it looks at the nature of the event as such and provides a brief overview on the institutional reactions and the debates that followed the cases. With regard to resilience, this section highlights the most important strategies that have been developed and implemented.

Nature of the adverse event

Between 2002 and 2009, the following school shootings took place in Germany. According to different sources, the numbers and events vary. Some are included on some lists, but not on others. The below list aims to be as inclusive as possible.

1. Eching und Freising, 19 February 2002: Adam Labus, 22 years old, killed four people including himself and injured one. In addition to his former school, he killed at his workplace.
2. Erfurt, 26 April 2002: Robert Steinhäuser, 19 years old, killed 17 people, including himself, at the Gutenberg-Gymnasium in Erfurt. This was considered to be the first school shooting in Germany, however, not the first disruptive shooting or killing spree in Germany.
3. Coburg, July 2003: Florian K., 16, injured his teacher and killed himself. This concerned a very personal issue; it is included as it was carried out in a school.
4. Emsdetten, 20 November 2006: Bastian B., 18, killed six people at his school, including himself. He threw petrol bombs; 32 children had to be treated for smoke poisoning.
5. Winnenden, 11 March 2009: Tim Kretschmer, 17, killed 15 people and himself after a car chase through the town. A further 11 people were injured.
6. Ansbach, 17 September 2009: Georg R., 18, injured two pupils heavily with an axe and seven others less seriously. He did not use guns, but petrol bombs, knives and an axe. He did not kill himself, but was shot (not killed), and eventually sentenced.

Prior to these, there were two other incidents worthy of mention due to their temporal proximity and similar modus operandi.

1. Meißen, Saxony, 9 November 1999: A 15-year-old pupil killed his teacher with a knife.

2. Brannenburg, Bayern: A 16-year-old pupil killed the headmaster of his school, where he had been dismissed a day earlier. The teacher was shot in the head and died six days later. The pupil suffered self-inflicted injuries.[449]

Although all of these events were local in their impact, the killings generated a nation-wide outcry each time, most prominently Erfurt in 2002, which was the most severe to date. After Winnenden in 2009, efforts for change, measures and the discussion gathered a momentum that previous events (not even Erfurt which arguably generated the most intense reaction and probably greatest shock) had not generated.

The most frequent questions asked about these events relate to their causes, i.e., what caused young men to engage in such rage and killing, and ultimately suicide? Other important questions related to whether such events could have been avoided and whether they can be avoided in the future.

Immediately after each event, the survivors, victims' families and friends were offered psychological help and financial aids to cope with the aftermath of the shock they had experienced. School shootings may seem less of a threat (comparing victim counts) than transport accidents but the impact of these events is quite profound.

School shootings have made an impact on how to deal with such events, and with the issues of school violence in general. Strategies to avoid similar events in the future have been developed and policies discussed to increase awareness and identify dangers. As most or all perpetrators had an easy access to weapons at home or were shooters themselves, new laws for the registration of weapons have been discussed. However, the outcomes here have been rather negligible, but worth mentioning nevertheless, as this may shed some light on the relation between surveillance and resilience to cope with potential future events of this kind. Issues identified as possible factors for such events include:

- Is weak regulation of gun ownership a possible cause?
- Are media and violence in computer games the source of such events?

These issues have been debated in all the major papers and the media as a whole. However, as with most of these events, the time span in which an event makes the headlines and is intensively discussed is typically rather short. The same is true of the attention of politicians; they soon move on to other items on their agenda. The basic and most prominent arguments made are the ones stated above. Beyond this, no major argument was brought forward, and hence of actual relevance.

Institutional response

The initial responses of policy-makers, the state and its agents can be said to be symbolic. Various politicians demanded intensified video surveillance at schools, new gun laws and better prevention. The most prominent demand was for a ban on violent

[449] The dates and details of the listed school shootings have been taken from Wikipedia. http://de.wikipedia.org/wiki/Amoklauf_an_einer_Schule#Deutschland; See also Die Welt, Ein Toter bei Amoklauf an Schule in Ludwigshafen, 18 February 2010. http://www.welt.de/vermischtes/article6448983/Ein-Toter-bei-Amoklauf-an-Schule-in-Ludwigshafen.html

computer games (so-called "killer" games) as politicians thought they were responsible for such events.[450]

Very few of the suggested measures have been realised. In January 2013, a national registry of weapons came into effect. This constitutes a novelty in Germany. Before the national registry, weapon and gun control was the responsibility of each of the 16 Bundesländer (Germany's federal states). Almost no communications existed between those registries, which in reality was delegated even further down to the communal level. This meant that all in all, 550 local administrations oversaw the registration of weapons and did not exchange their data. Gun control was not an issue seen to require central control, but remained local and hence uncontrollable for a long time. After Winnenden event in 2009, German gun law was amended, resulting in new regulations on how and where private owners could and should store their weapons and guns. The registry is part of this process. The national registry has helped to determine the number of privately held weapons in Germany, which is 5.5 million, with 1.4 million registered owners[451]. At this stage, it is hard to say if the new national registry will prevent school shootings.

In addition, the Bundesverfassungsgericht (Federal Constitutional Court) ruled on 23 January 2013 that privately owned, high calibre weapons are still legal after relatives of the victims killed in Winnenden in 2009 filed an action against the ownership of such weapons. The court stated that the ban of such weapons would not prevent similar events in the future. However, the amended gun laws now treat infringements against the regulations as a crime and no longer as a regulatory offence. High calibre weapons may only be bought by adults over 21 years of age. [452]

It is important to note that the measures now in effect had already been discussed in 2002 after the first and most severe school shooting. However, it took a couple of more events before the establishment of a national weapons registry and amendment of the gun law. In 2002, the government of Thuringia, the state in which the city of Erfurt lies, stated that just because of one such horrific event, one could not put two million shooters pursuing a sport under general suspicion.[453] Seen in light of the anti-terror laws passed in Germany without an act of terror in the last 20 years and especially in the aftermath of 9/11, this attitude of denial is remarkable and very revealing. While it is assumed that most gun owners are law-abiding citizens, the Muslim population and other opposition figures and movements have met far greater and often general suspicion.

Societal response

[450] Spiegel Online, "Reaktionen auf Amoklauf: Politiker fordern nach Schul-Blutbad Konsequenzen, " *Spiegel Online*, 11 March 2009. http://www.spiegel.de/politik/deutschland/reaktionen-auf-amoklauf-politiker-fordern-nach-schul-blutbad-konsequenzen-a-612721.html

[451] Bundesministerium des Inneren, "Das Vorhaben "Nationales Waffenregister"" 1 January 2013. http://www.bmi.bund.de/DE/Themen/Sicherheit/Waffenrecht/Nationales-Waffenregister/nationales-waffenregister_node.html

[452] Bundesverfassungsgericht, Pressemitteilung Nr. 8/2013, 15 February 2013, Beschlüsse vom 23 January 2013, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg13-008.html

[453] Robertz, Frank, *School Shootings. Über die Relevanz der Phantasie für die Begehung von Mehrfachtötungen durch Jugendliche*, Verlag für Polizeiwissenschaft, Frankfurt/Main, 2004.

The responses with the most impact on prevention and understanding were, did not come from the state or policy-makers, but from civil society and academia. Academic departments of the police are subsumed under academia in this case, as it is closer to what they do than law-making or policy development.

Social responses can be classified into a two different approaches:

- Research
- Prevention

Helping the survivors coping with their trauma may be seen as a third aspect, but constitutes a very personal and potential problem. Trauma counselling is often uncoordinated, random and often a cause for further damage more than an appropriate handling of traumatic experiences. ötz Eisenberg, prison psychologist, states in a commentary on the trauma industry that 40 years ago such an industry did not exist and people were left alone[454]. He suggests that something he calls the "social immune system" was still intact and dealing with trauma was not an individualised issue. Without discussing this aspect much further, this may constitute an area where research into resilience should also be looking, i.e., the history of resilience strategies (whether by using this term of not). This short report does not take into account this aspect in favour of a deeper analysis of the responses aimed at future events. Both aspects – research and prevention – are interlinked, as much research has been conducted to explore the causes in order to find new ways of prevention.

In addition to the uncountable number of newspaper and magazine articles published in the last 11 years on the subject of school shootings, a few initiatives, research projects and active measurements emerging from these events stand out. The common ground on which all of these projects and measurements are built is that very little is known about school shootings, the perpetrators themselves and whether from such knowledge it is possible to find ways to stop potential shooters.

The largest project of this kind was NETWASS – Network against School Shootings – based at the Freie Universität Berlin. The project aimed to develop early warning systems concerning psycho-social states of emergency among pupils. More than 100 schools in three Bundesländer in Germany and roughly 5,000 teachers took part. The project concluded in 2013 and was followed by TARGET – Tat- und Fallanalysen hochexpressiver zielgerichteter Gewalt (Case Analyses of highly expressive and goal-oriented violence). While NETWASS aimed at developing preventive measures, TARGET aims to gather insights from a comparative analysis of various events with a view to prevent further attacks. NETWASS was oriented on actual work in schools, developing models that address all concerned parties – pupils, teachers and parents. TARGET is more academic and only started in spring 2013, so nothing can be said about the results yet.

Other research on this subject has appeared on a much smaller scale in reports or academic theses.[455] One overall finding that has emerged from various documents,

[454] Eisenberg, Götz, "Industrialisierung des Mitleids," *Der Freitag*, 19 March 2009. http://www.freitag.de/autoren/der-freitag/industrialisierung-des-mitleids

[455] The following list provides an overview of research, guidelines and academic analysis: Robertz, Frank, *School Shootings. Über die Relevanz der Phantasie für die Begehung von Mehrfachtötungen durch Jugendliche*. Verlag für Polizeiwissenschaft, Frankfurt/Main, 2004; Amoktaten –

especially those strictly concerned with preventive aspects or guidelines, is that there is no true checklist to actually prevent such events from happening. The reasons and factors that lead to such events are too diverse and specific than can be covered by an overall fitting checklist. As with all classification systems, anything that classifies perpetrators or provides indicators of events about to happen risks producing false positives.

Overall, it can be said that the social responses aim to prevent such events from recurring. One focus has been on social and preventive work in schools, educating teachers, establishing early warning systems and fostering a communal understanding and care among pupils, between pupils and teachers, and involving the parents at various stages.

Surprisingly, little attention has been given to the implementation of technical devices such as video surveillance, metal detectors or human security, i.e., security personnel, at schools. All discussion involving such demands were met with great suspicion and died down very quickly. One rather technical response is the so-called Farbleitsystem (a colour-coded guidance system[456]), with which schools in Germany are successively equipped. With the guidance system rescue teams, police, firemen and others can find their way in schools much more easily. They do not have to know anything about the schools, but can follow the colours. In the case of a school shooting or an attempted attack, help may be better organised and the actual attack even prevented. Together with other preventive measures laid out in the "2012: Amoklauf an Schulen"[457] document, such a system may help to strengthen schools and ensure safety and security. The colour code system classifies different areas of a building or site by colour. Emergency personnel do not have to find a particular room by number, e.g., room A4 or the art class, but can be guided by asking for help in the yellow area. Signage and colours will lead the way. The colours make it easier for emergency officials to ask for help without much explanation. The colour code system provides a standardised system of classifying a building, hence all orientation is pre-conditioned without the need of expert or local knowledge in the case of an emergency, not only in the case of school shootings, but also in the case of fires or other hazardous incidents. The colour code provides a visible and readable map imprinted on the building itself.

In addition to measures concerned with the specific event of a school shooting, research projects such as NETWASS also focus on issues of violence in schools more generally. Therefore, this adverse event has stimulated an awareness of other possible forms of violence among pupils in a school environment. The current strategy is to find ways to prevent this kind of violence and raise the general sensitivity and

---

Forschungsüberblick unter besonderer Beachtung jugendlicher Täter im schulischen Kontext, Kriminalistisch-Kriminologische Forschungsstelle Analysen Nr. 3/2007, Landeskriminalamt NRW, 2007; Kühling, Anne, *Ursachen und Hintergründe zu extremen Gewalttaten an deutschen Schulen,* Vechtaer Verlag für Studium, Wissenschaft und Forschung, 2009; Siegel, Birgitt, "Amoklauf an Schulen", Verband der Lehrerinnen und Lehrer an Wirtschaftsschulen in NRW e.V., 2012. NETWASS has published numerous articles and guidelines on its website: http://www.ewi-psy.fu-berlin.de/v/netwass/index.html.

[456] Das Farbleitsystem (FLS). http://farbleitsystem.de. See also: http://www.praeventionstag.de/nano.cms/rund-um-den-dpt

[457] Siegel, Birgitt, "Amoklauf an Schulen", Verband der Lehrerinnen und Lehrer an Wirtschaftsschulen in NRW e.V., 2012

awareness among pupils, teachers and parents. Almost all strategies initiated following the events of the last 10 years aim to foster a sense of community and care for each other.

Conclusions from an IRISS perspective

School shootings have dominated public discourse when they occurred. Even when they happened elsewhere in the world, such as in Newtown in 2012, past events re-surfaced and discussions re-emerged in Germany[458]. Events such school shootings are not avoidable; they happen suddenly, although research has shown that in contrast to terrorist attacks, there are more visible signs and sometimes even announcements by the potential shooters before such events. Hence, prevention may be an option, which is never the case with terrorists. Prevention in the case of terrorist attacks is primarily the responsibility of intelligence services, as are clandestine measures and many measures that citizens experience as surveillance. In the case of school shootings, such measures have mostly been neglected in favour of more socially and community-oriented approaches. Human factors, rather than technology, have been identified as the major source of prevention.

However, if we take community and its role in social control, then surveillance in the widest sense is acted out in very classical forms. It would be too simple to state that resilience has been achieved by increased social control and mutual surveillance among pupils. All approaches and the accompanying research aim to strengthen the bonds among pupils, deter social exclusion and raise awareness. Schools will always be vulnerable, because they are open spaces – a pre-requisite for a culture and environment of learning that are highly valued among German parents. Following the events – albeit not right away – there have been measures in the political arena supporting societal responses in that they are trying to decrease the danger of legally held weapons through regulatory schemes. Whether this is the end, and solution to the problem remains to be seen. As with other attacks, especially terrorist attacks, all it takes is a will to do something, no matter what the locks and laws are.

School shootings seem to have generated the insight that "the social immune" system is degrading and has to be strengthened in order to prevent future similar attempts. Whether strategies that identify video games or other secondary aspects as root causes are a good way forward in the discussion, are debatable. The research projects and active engagement of schools have proven that other ways are more effective and able to take more people on board.

In this case, it seems as if communal self-organisation together with support from state agencies and research institutions are more successful than populist demands for more surveillance, new technologies or other security measures that are rather associated with terrorist attacks. Open environments such as schools have to be supported in their nature to be open. This in not to say that all has to be possible, but more restraints do not seem to be a way forward, rather, they are arguably part of the problem.

---

[458] Winkelsdorf, Lars, "Muss auch Deutschland das Waffenrecht verschärfen?, " *Der Tagesspiegel*, 18 December 2012. http://www.tagesspiegel.de/politik/nach-dem-amoklauf-von-newtown-muss-auch-deutschland-das-waffenrecht-verschaerfen/7533612.html

References

Books

Bannenberg, B., Amok, *Ursachen erkennen - Warnsignale verstehen - Katastrophen verhindern,* Gütersloher Verlagshaus, Gütersloh, 2010.

Bond, Rebecca and Herbert Scheithauer, *Amoklauf und School Shooting: Definition, Verbreitung, Hintergründe und Prävention*, Vandenhoeck & Ruprecht, Göttingen, 2011.

Faust, Benjamin, *School-Shooting. Jugendliche Amokläufer zwischen Anpassung und Exklusion,* Psychosozial-Verlag, Gießen, 2010.

Gräf, Angela, and Joachim Grösbrink, *Frau komA kommt. Amok an Schulen: Über Täter und Opfer,* Deutsche Polizeiliteratur, 2011.

Robertz, Frank, and Ruben Wickenhäuser, *Der Riss in der Tafel. Amoklauf und schwere Gewalt in der Schule*. Springer, Heidelberg, 2007.

Robertz, Frank, *Über die Relevanz der Phantasie für die Begehung von Mehrfachtötungen durch Jugendlich*e, Verlag für Polizeiwissenschaft, Frankfurt, 2004.

Academic articles

Albrecht, Richard, "Nur ein 'Amokläufer'? − Sozialpsychologische Zeitdiagnose nach Erfurt", *Recht und Politik*, Vol. 38, No. 3, 2002, pp. 143-152.

Bondü, R., S. Meixner, H.D, Bull, F. Robertz, and H. Scheithauer, H. Schwere, "Zielgerichtete Schulgewalt: School Shootings und Amokläufe", in H. Scheithauer, T. Hayer and K. Niebank (eds.), *Problemverhalten und Gewalt im Jugendalter. Erscheinungsformen, Entstehungsbedingungen, Prävention und Intervention,* Kohlhammer-Verlag, Stuttgart, 2008.

Bondü, R. and H. Scheithauer, "School Shootings in Deutschland: Aktuelle Trends zur Prävention von schwerer, zielgerichteter Gewalt an deutschen Schule, Praxis", *Kinderpsychologie und Kinderpsychiatrie*, Vol. 58, 2009, pp. 685-701.

Heubrock, D., T. Hayer, S. Rusch, and H. Scheithauer, "Prävention von schwerer zielgerichteter Gewalt an Schulen – Rechtspsychologische und kriminal-präventive Ansätze", *Polizei & Wissenschaft,* 1/2005, pp. 43-45.

Harnischmacher, Robert F. J., "Gewalt an Schulen: Das Amok-Phänomen", *Kriminalpolizei. Zeitschrift der Gewerkschaft der Polizei*, Undated.
http://www.kriminalpolizei.de/weitere-rubriken/kapitaldelikte/detailansicht-kapitaldelikte/artikel/gewalt-an-schulen-das-amok-phaenomen.html

Hoffmann, J., "Amok - ein neuer Blick auf ein altes Phänomen", in C. Lorei (ed.), *Polizei und Psychologie, Proceedings of the conference on 'Polizei & Psychologie'*, Verlag für Polizeiwissenschaft, Frankfurt am Main, 2003, pp. 397-414.

Scheithauer, Herbert, and Dietmar Heubrock, "Gewalt an deutschen Schulen. Präventives Eingreifen als Lebensretter", *Fundiert. Das Wissenschaftsmagazin der FU Berlin*, 2005.
http://www.elfenbeinturm.net/archiv/2005/11.html

Wieczorek, Arnold, "Schülerattentate an deutschen Schulen. Mythen, Fakten und Schlussfolgerungen für die polizeiliche Praxis", *Kriminalistik*, Vol. 64, 2010, pp. 153ff.

3.2.7 2011 Christchurch earthquake

Charles Leleux, University of Stirling

Nature of the adverse event

Located on the South Island of New Zealand, and sitting within the Canterbury region, the city of Christchurch (population: 341,000) is the country's second largest city.[459] Originally inhabited by the indigenous Maori populations, the first Europeans were thought to have settled in what became Christchurch in the early 1840s, with their original trades being whaling and farming.[460] The Mw6.3 earthquake which hit Christchurch unexpectedly and catastrophically on 22 February 2011 at 12.51 killed over 180 people, injured a further 1500-2000, and was in fact an aftershock of a previous earthquake (Mw7.1) occurring on 4 September 2010 which resulted in no fatalities.[461] The Canterbury Television (CTV) building which collapsed resulted in the loss of 115 lives. After the earthquake on 22 February 2011 it was estimated that 800 business premises in the central business district (CBD), where most of the fatalities occurred, plus 10,000 domestic properties would require to be demolished, and that the economic costs of repairing the damage would be in the region of US $11-15 billion.[462] Most of the fatalities were caused by soil liquefaction leading to lateral movement of buildings, tilting of buildings, falling masonry and collapse of both reinforced and unreinforced buildings.[463] An extensive study of the performance of masonry buildings and churches was commissioned in March 2011, i.e. the month following the earthquake, by the New Zealand Natural Hazards Research Platform, and recommendations from the subsequent report later that year, included "appropriate seismic retrofit and remediation techniques for stone masonry

[459] Statistics New Zealand, 2013 Census of Population and Dwellings. http://www.stats.govt.nz/Census/2013-census/data-tables/population-dwelling-tables.aspx
[460] Christchurch City Council, "History". http://www.christchurch.org.nz/about/history.aspx
[461] Reyners, Martin, "Lessons from the destructive Mw 6.3 Christchurch, New Zealand, earthquake", *Seismological Research Letters*, Vol. 82, No. 3, 2011, pp. 371-372.
[462] Ibid.
[463] Cubrinovski, Misko, Jonathan D. Bray, Merrick Taylor, Simona Giorgini, Brendon Bradley, Liam Wotherspoon, and Joshua Zupan, "Soil liquefaction effects in the central business district during the February 2011 Christchurch earthquake", *Seismological Research Letters* Vol. 82, No. 6, 2011, pp. 893-904.

buildings".[464] A Royal Commission was also established to investigate the reasons for building failure, due to the two earthquakes, and sat between 2011 and 2012, making various recommendations regarding the future preparation of regional and district plans, and the need for greater involvement of structural engineers and geotechnical surveys at the planning stages of applications for construction projects. The main difference between the Christchurch earthquakes of September 2010 and February 2011, was that the former event occurred out with the CBD area, and although very powerful and causing much damage, the epicentre of the latter event was fairly close to the CBD, causing many buildings to collapse with subsequent loss of life.[465]

Awareness amongst public bodies of the likelihood of ground movements and earthquakes in this area was high, although the September 2010 and February 2011 earthquakes occurred on fault lines which the authorities were not aware of, occurring on "……previously unknown fault lines in a region of historically low seismicity but within the zone of plate boundary deformation between the Pacific and Australian plates".[466] Pettinga et al, record that there are around ninety major earthquake source faults around the Canterbury region, which includes Christchurch, and characterise these faults according to "type (sense of slip), geometry (fault dimensions and attitude) and activity (slip rates, single event displacements, recurrence intervals, and timing of last rupture)".[467] Pettinga et al also provide an historical account of earthquakes taking place in Christchurch and the wider Canterbury region, notably those taking place in 1869, 1870, 1888, 1902, 1922, 1929 and 1994.[468] Various regional, national and international monitoring systems were already recording on a daily basis, any changes in ground conditions and seismological activity, and various modelling techniques were also in use to predict the likelihood and frequency of such a major event taking place.[469] The Christchurch earthquake of 22 February 2011, which was not predicted by the scientific community (although there were significant ground movements recorded), was the worst to hit New Zealand since the Hawkes Bay earthquake in 1931.[470] The Mw7.8 earthquake which took place on 2 February 1931 at Hawkes Bay on the North Island, severely damaged two towns, Napier and Hastings, and resulted in the loss of 256 lives, with the surrounding area suffering

[464] Dizhur, Dmytro, Jason Ingham, Lisa Moon, Mike Griffith, Arturo Schultz, Ilaria Senaldi, Guido Magenes et al, "Performance of masonry buildings and churches in the 22 February 2011 Christchurch earthquake", *Bulletin of the New Zealand Society for Earthquake Engineering*, Vol. 44, No. 4, December 2011, pp. 279-295.
[465] Ibid.
[466] Beavan, John, Eric Fielding, Mahdi Motagh, Sergey Samsonov, and Nic Donnelly, "Fault location and slip distribution of the 22 February 2011 Mw 6.2 Christchurch, New Zealand, earthquake from geodetic data" *Seismological Research Letters*, Vol. 82, No. 6, 2011, pp. 789-799.
[467] Pettinga, Jarg R., Mark D. Yetton, Russ J. Van Dissen, and Gaye Downes, "Earthquake source identification and characterisation for the Canterbury region, South Island, New Zealand", *Bulletin of the New Zealand National Society for Earthquake Engineering,* Vol. 34, No. 4, 2001, pp. 282-317.
[468] Ibid.
[469] Cubrinovski, Misko, Jonathan D. Bray, Merrick Taylor, Simona Giorgini, Brendon Bradley, Liam Wotherspoon, and Joshua Zupan, "Soil liquefaction effects in the central business district during the February 2011 Christchurch earthquake", *Seismological Research Letters,* Vol. 82, No. 6, 2011, pp. 893-904.
[470] Kaiser, A., C. Holden, J. Beavan, D. Beetham, R. Benites, A. Celentano, D. Collett et al, "The Mw 6.2 Christchurch earthquake of February 2011: Preliminary report," *New Zealand Journal of Geology and Geophysics,* Vol. 55, No. 1, 2012, pp. 67-90.

aftershocks and further earthquakes in the weeks and months following.[471] The extent to which the local community, local agencies and national bodies demonstrated their resilience both prior to and following the event on 22 February 2011 including the use of any surveillance technologies, is examined in the following sections.

Institutional response

In the immediate aftermath of the earthquake on 22 February 2011 responsibility for control of the areas affected fell to John Hamilton, the Director of Civil Defence Emergency Management,[472] who established communications with the National Crisis Management Centre in Wellington, the local Civil Defence and Emergency Management Group in Christchurch, and Christchurch City Council. The Ministry of Civil Defence and Emergency Management responded quickly by issuing a fairly short but purposeful media release at 15.30 on 22 February (only two hours and forty minutes after the earthquake struck). The media release advised people on where the earthquake was centralised; the operational status of Christchurch hospital and the airport, plus made suggestions about keeping cellphone usage to a minimum as the network was struggling due to heavy demand from people trying to contact loved ones; avoiding travelling by road unless absolutely necessary, and encouraging people to keep updated by listening to local radio and Radio New Zealand.[473] Further advice was also provided in the same media release about personal safety in and around the home, paying particular attention to utility services, including links to various websites. The Ministry of Civil Defence and Emergency Management issued additional media releases on 23 February providing a Red Cross Person Enquiry Helpline, and on 24 February on how to make cash donations to help people affected by the disaster:

> The Ministry of Civil Defence & Emergency Management is stressing that cash donations are the best way to support people affected by the Canterbury earthquake.[474]

The New Zealand Government declared a State of National Emergency on 23 February 2011; this lasted for nearly nine weeks. The Government also acted with impressive speed in passing the Canterbury Earthquake Recovery Act 2011 on 18 April 2011 less than two months after the event, the purposes of which included not only the physical rebuilding of properties and infrastructure, but also the rebuilding of social capital:

> (a) to provide appropriate measures to ensure that greater Christchurch and the councils and their communities respond to, and recover from, the impacts of the Canterbury earthquakes
> (b) to enable community participation in the planning of the recovery of affected communities without impeding a focused, timely, and expedited recovery

---

[471] Eiby, G. A., "An annotated list of New Zealand earthquakes, 1460–1965", *New Zealand Journal of Geology and Geophysics,* Vol. 11, No. 3, 1968, pp. 630-647.
[472] Ministry of Civil Defence & Emergency Management. http://www.civildefence.govt.nz/
[473] Ministry of Civil Defence & Emergency Management. http://www.civildefence.govt.nz/memwebsite.nsf/wpg_URL/Media-Media-release-archive-Index?OpenDocument
[474] Ibid.

(c) to provide for the Minister and CERA (Canterbury Earthquake Recovery Agency) to ensure that recovery
(d) to enable a focused, timely, and expedited recovery
(e) to enable information to be gathered about any land, structure, or infrastructure affected by the Canterbury earthquakes
(f) to facilitate, co-ordinate, and direct the planning, rebuilding, and recovery of affected communities, including the repair and rebuilding of land, infrastructure, and other property, and
(g) to restore the social, economic, cultural, and environmental well-being of greater Christchurch communities.[475]

CERA[476] was established by the New Zealand Government through the Canterbury Earthquake Recovery Act 2011 shortly after the earthquake to work closely with other agencies, such as regional, city and district councils, and in particular Christchurch City Council (CCC).[477] Primary responsibilities of CERA included governance; infrastructure coordination and planning; planning and deconstruction of buildings (jointly in many cases with CCC); economic recovery coordination; skills and workforce planning, and welfare rebuild coordination. A formal Cost Sharing Agreement was also put in place between the Crown and CCC. The extent to which tensions emerged between the various agencies, and in particular CERA and CCC, in the course of inter-agency working, is examined under the section 'Economic Response'.

The Canterbury Earthquakes Royal Commission was established to report on the causes of building failure as a result of the earthquakes as well as the legal and best practice requirements for buildings in New Zealand Central Business Districts. The Inquiry began in April 2011 and was completed in November 2012. The Chair of the Royal Commission, Justice Mark Cooper gave the following commitment to those affected by the disaster, "Those who lost relatives and friends in the 22 February earthquake can be assured that there will be a very thorough inquiry into the failure of buildings that resulted in loss of life".[478]

The Royal Commission produced their report in three parts, with some of the key recommendations including: regional and district plans to be prepared on the basis that they acknowledge the potential effects of earthquakes and liquefaction; regional and district authorities to be adequately informed about seismicity of their regions and districts; applicants must ensure geotechnical and structural engineering information is provided from professionally qualified persons, and greater powers for councils to ensure the involvement of structural engineering experts in the planning application process.

Societal Response

[475] New Zealand Parliament, Canterbury Earthquake Recovery Act 2011. http://legislation.govt.nz/act/public/2011/0012/latest/DLM3653522.html?src=qs
[476] CERA, Canterbury Earthquake Recovery Agency. http://cera.govt.nz/about-cera/roles-and-responsibilities
[477] Christchurch City Council. http://ccc.govt.nz/Content/Search/SearchResults.aspx?query=christchurch+earthquake&btnG=Search
[478] Canterbury Earthquakes Royal Commission. http://canterbury.royalcommission.govt.nz/

Turning firstly to the argument that society perhaps contributed in some way to the effects of the Christchurch disaster of 22 February 2011, it could not reasonably or justifiably be claimed that the city and its surrounding environment were formed in a place which is susceptible to such an event, and therefore society could be blamed in part for the consequences of this naturally occurring event. As outlined in the previous section, although there were numerous known geological faults in the wider Canterbury region, with several recorded earthquake events occurring in the previous century, and with daily monitoring of ground conditions taking place, the two earthquakes which took place in September 2010 and February 2011 occurred on geological fault lines which were unknown to the scientific community. The catastrophic earthquake which occurred on 22 February 2011 caused damage, destruction and fatalities on a scale unrecorded in Christchurch previously, did so despite the seismological technology at the disposal of the scientific community.

Regarding the resilience of the built environment, it is clear from studies which have been undertaken that it was not sufficient enough to withstand the effects of the earthquake, in particular in the CBD. Both reinforced and unreinforced office buildings collapsed or were damaged as a result of which people lost their lives. In particular, the Canterbury Television building (CTV) which collapsed, resulted in the loss of 115 lives. The technical study commissioned by the New Zealand Natural Hazards Research Platform involved an international team of scientists who documented and interpreted the destruction and damage to over 2000 buildings which were both reinforced and unreinforced, including churches, commercial and domestic properties. They investigated the failure patterns and collapse mechanisms that were commonly encountered, and found unsurprisingly that unreinforced buildings sustained far greater damage than reinforced ones. The findings concluded:

> that when subjected to the higher forces generated by the earthquake on 22nd February 2011, Christchurch's unreinforced masonry building stock sustained much greater and more widespread damage than in the 4th September 2010 earthquake. Cases of severe structural damage to RCM (reinforced concrete masonry) buildings were found in the vicinity of the CBD. Structural damage to these buildings has been documented and is currently being studied to establish the lessons which can be learned from this earthquake and how to incorporate these lessons into future RCM design and construction.[479]

The extensive technical recommendations of the Royal Commission[480] include improving the geotechnical information available for building sites; far greater involvement of structural engineers in the planning process, and greater information to be available to the relevant authorities on seismicity of regions and districts. Significantly, the study did not document the performance of reinforced buildings against unreinforced ones in terms of numbers of lives lost.

Turning to examples the development of social capital, New Zealand Tourism has promoted positive upbeat messages, reflecting the resilience of the city and its people, following the earthquake to encourage tourists to continue to visit Christchurch:

---

[479] Dizhur, Dmytro, Jason Ingham, Lisa Moon, Mike Griffith, Arturo Schultz, Ilaria Senaldi, Guido Magenes et al, "Performance of masonry buildings and churches in the 22 February 2011 Christchurch earthquake", *Bulletin of the New Zealand Society For Earthquake Engineering*, Vol. 44, No. 4, December 2011, pp. 279-295.

[480] Canterbury Earthquakes Royal Commission. http://canterbury.royalcommission.govt.nz/

> The city has bounced back after a series of earthquakes, and all public services and spaces are running as normal.[481]
>
> The buildings may have been damaged but the soul of the city and the welcoming spirit of the people remain very much intact. Don't miss visiting Christchurch.[482]

The University of Canterbury created the CEISMIC Programme (Canterbury Earthquake Images, Stories and Media Integrated Collection) to provide access to a broad range of earthquake-related research material, gathered by leading New Zealand cultural and educational organisations:

> Our task now is to increase the content available through UC CEISMIC search, and ensure it is safeguarded for future generations. We've cast a net over our cultural heritage community to give the people of Christchurch and New Zealand a single place to create, remember and research their heritage, but we need your help to build it. You're also invited to contribute to our efforts.[483]

A Christchurch local resident, Adam Hutchison created the website whenmyhomeshook.co.nz[484] for children to record and openly share their earthquake stories. These accounts may become part of the UC CEISMIC archive. The New Zealand Ministry of Civil Defence & Emergency Management in their media release on 22 February 2011 called on citizens to assist vulnerable people who may need help due to the effects of the earthquake, "help people who require special assistance - infants, elderly people, those without transportation, large families who may need additional help, people with disabilities, and the people who care for them". [485]

CERA, in a press release on 18 March, 2014, provided results of the Third Canterbury Earthquake Recovery Authority Wellbeing Survey, with 2,476 residents being selected randomly from the electoral roll in Christchurch city, and the surrounding districts of Selwyn and Waimakariri, with around 75% of Greater Christchurch residents being satisfied with the positivity of their life: It stated, "overall three quarters of Greater Christchurch residents rate the quality of their life positively, which remains consistent with surveys taken in September 2012 and April 2013."[486]

CERA chief executive Roger Sutton is quoted as saying that the results show that the earthquakes are now having less of an impact on many residents' lives than six months ago. "While most respondents do acknowledge there are areas of their lives which are still affected by the earthquakes, the focus has changed. We used to hear about the anxiety people felt about aftershocks, dealing with frightened children and

[481] New Zealand Tourism. http://www.newzealand.com/uk/christchurch/
[482] New Zealand Tourism. http://www.newzealand.com/uk/christchurch-canterbury/
[483] University of Canterbury. http://www.ceismic.org.nz/
[484] http://whenmyhomeshook.co.nz/
[485] Ministry of Civil Defence & Emergency Management. http://www.civildefence.govt.nz/memwebsite.nsf/wpg_URL/Media-Media-release-archive-Index?OpenDocument
[486] CERA. http://cera.govt.nz/news/2014/secondary-stressors-now-a-larger-factor-for-earthquake-affected-residents-18-march-2014

work safety concerns." "Those stressors are being replaced with frustrations about traffic, and other work-related issues."[487]

CERA's webpages provide an extensive range of links to assist members of the public and communities. The community resilience webpage contains positive language specifically directed towards recovering from the earthquakes:

> Community resilience requires participation from the whole community to improve response and recovery, and to help the community plan for the future. The impact and effect of the earthquakes have been different for each and every one of us. As a wider community we are all in this together. It's important that we continue to champion the strong sense of community that helped us manage and move forward following the earthquakes. [488]

Economic response

In the media release issued on 24 February 2011 the Ministry of Civil Defence and Emergency Management directed advice to local businesses who were keen to offer expertise, and to people wishing to volunteer, who were advised to wait, and not to send employees or resources or to go to Christchurch themselves. Instead, they were advised, "when local authorities have a clear idea of what is needed and are in a position to manage goods and volunteers they will advise publicly what is needed and where."[489]

Responsibility for economic recovery coordination and skills/workforce planning fell to CERA, working in partnership with local, city and regional councils and other agencies. The Canterbury Economic Recovery Dashboard provided monthly updates on the earthquake recovery in Christchurch.[490] The latest published dashboard report, August 2013, supplied information represented in graphs, including the following areas, most of which showed an upward trajectory of growth and improvement: output, consumer spend, agriculture, manufacturing, services, tourism, investment, housing, insurance, business development, population, employment, and spending.[491]

CERA, as part of the Canterbury Earthquake Recovery project, is using a Better Business Case model to consider projects and programmes requiring Crown investment in whole or in part. The model is based on five key cases: strategic, economic, commercial, financial and management, and overall how the case meets the recovery strategy. Funding decisions are then made after an evaluation of the respective business cases.[492] The Canterbury Economic Indicators Quarterly Report, August 2013 gives a more in-depth analysis of the economic recovery and response, as evident in the following upbeat summary:

---

[487] Ibid.
[488] CERA. http://cera.govt.nz/community-resilience
[489] Ministry of Civil Defence & Emergency Management. http://www.civildefence.govt.nz/memwebsite.nsf/wpg_URL/Media-Media-release-archive-Index?OpenDocument
[490] CERA. http://cera.govt.nz/economic-indicators
[491] CERA. http://cera.govt.nz/sites/cera.govt.nz/files/common/canterbury-economic-recovery-dashboard-august-2013.pdf
[492] CERA. http://cera.govt.nz/better-business-cases

> The Canterbury economy continues to grow and consumer confidence remains steady. International and domestic tourism is returning to pre-earthquake levels and more taxpayers are migrating into greater Christchurch than migrating out. Commercial investment remains significantly more optimistic for Canterbury than for the rest of New Zealand: greater Christchurch has been the most confident commercial property investment market every quarter since 2011, according to Colliers International results of June 2013. However, such high rates of growth present challenges as well as opportunities. Noticeably, house prices and rents are rising steadily. The higher demand in the labour market is putting pressure on employers who are having difficulties in finding skilled labour.[493]

The economic response appears to have been successfully managed and coordinated by CERA as the previous summary from the Canterbury Economic Indicators Report demonstrates. Undoubtedly, achieving this level of sustained progress will have been dependent upon very high levels of capital funding, inter-agency working and co-operation, however, however the position is unclear regarding the success of inter-agency co-operation. There have been tensions between the various agencies or personalities working within them during the renewal process, and in particular between CERA and Christchurch City Council (CCC), a fact acknowledged by CERA Chief Executive, Roger Sutton. In responding to criticism that the rebuild was taking too long, Sutton admitted that the rebuild was a bigger project than he initially thought and that relationships with the government and local council had at times been volatile:

> When asked about the strained relationship between CERA and the Christchurch City Council, Mr Sutton said: "We'd like to think that we're here to make it work, we're here to help and we're trying to support this community'''.[494]

Most likely, these tensions will have come to prominence over the uncomfortable fit between the democratically elected city council with their agreed governance procedures for consultation, decision making and accountability, and the more direct decision making processes employed by CERA. Tensions between CERA and CCC also surfaced over the city's housing shortages, with the two bodies committing to work together to address the problem, which has driven up rents and house prices, with the problem predicted to worsen up until 2017:

> I would like to think this is a new start . . . that we can work together. There is so much at stake," council housing committee chairman Cr Glenn Livingstone said yesterday (27.11.13).'[495]

Critical conclusions from an IRISS perspective

- Surveillance technologies were deployed extensively to monitor ground movements and other seismological activity, however the earthquake on 22 February, 2011 was not predicted by the scientific community and occurred on a previously unnown fault line;

---

[493] CERA, "Canterbury Economic Indicators", August 2013. http://cera.govt.nz/sites/cera.govt.nz/files/common/canterbury-economic-indicators-quarterly-report-august-2013.pdf

[494] TVNZ. http://tvnz.co.nz/national-news/christchurch-rebuild-balancing-act-cera-5846679

[495] Cairns, Lois, "Housing pinch to worsen until 2017", *The Press,* 27 November 2013. http://www.stuff.co.nz/the-press/business/your-property/9446008/Housing-pinch-to-worsen-until-2017

- The resilience of the built environment, particularly in some parts of the central business district, was found not to be have been sufficient enough to withstand the effects of the earthquake, and lessons learned from both an extensive survey and a Royal Commission Inquiry will used for future RCM (reinforced concrete masonry) design and construction; regional and district planning, supply of geotechnical and seismological information, and greater use of structural engineering information and expertise in planning application processes;
- The immediate institutional response in terms of media communications was informative, practical and appropriate, and a state of emergency was declared the day following the event by the New Zealand Government, continuing for around nine weeks;
- The enduring institutional response saw the passing of an Act of Parliament, within two months of the disaster, and the creation of a dedicated agency: the Canterbury Earthquake Recovery Agency (CERA), which is continuing to support both the physical rebuild of properties and infrastructure, and the social capital of the Canterbury region and Christchurch city;
- The resilience of the agencies involved in the rebuild of the physical, economic and social infrastructure is clearly evident and successful according to the Canterbury Economic Indicators Report (August 2013), however there have been criticisms that the rebuild is too slow, and there is evidence of tensions and volatility in particular between CERA and CCC, and
- The rebuilding of social capital has been extensive and has involved many agencies working on different aspects, including keeping channels open for communities and individuals including children to record their 'stories' such as oral history projects, and in particular the CEISMIC project established by the University of Canterbury whose objective is collect material relating to the earthquake and to give the people of Christchurch and New Zealand a single place to create, remember and research their heritage.[496]

References

Beavan, John, Eric Fielding, Mahdi Motagh, Sergey Samsonov, and Nic Donnelly, Fault location and slip distribution of the 22 February 2011 Mw 6.2 Christchurch, New Zealand, earthquake from geodetic data, *Seismological Research Letters* 82, no. 6, 2011, pp789-799.

Canterbury Earthquakes Royal Commission. http://canterbury.royalcommission.govt.nz/

CERA, Canterbury Earthquake Recovery Agency. http://cera.govt.nz/about-cera/roles-and-responsibilities

CERA. http://cera.govt.nz/news/2014/secondary-stressors-now-a-larger-factor-for-earthquake-affected-residents-18-march-2014

CERA. http://cera.govt.nz/community-resilience

[496] The author is indebted to Elizabeth Eppel of the University of Wellington, NZ for her kind assistance.

CERA. http://cera.govt.nz/economic-indicators

CERA. http://cera.govt.nz/sites/cera.govt.nz/files/common/canterbury-economic-recovery-dashboard-august-2013.pdf

CERA. http://cera.govt.nz/sites/cera.govt.nz/files/common/canterbury-economic-indicators-quarterly-report-august-2013.pdf
CERA: http://cera.govt.nz/better-business-cases

Christchurch City Council. http://www.christchurch.org.nz/about/history.aspx

Christchurch City Council. http://ccc.govt.nz/Content/Search/SearchResults.aspx?query=christchurch+earthquake&btnG=Search

Cubrinovski, Misko, Jonathan D. Bray, Merrick Taylor, Simona Giorgini, Brendon Bradley, Liam Wotherspoon, and Joshua Zupan, "Soil liquefaction effects in the central business district during the February 2011 Christchurch earthquake", *Seismological Research Letters,* Vol. 82, No. 6, 2011, pp. 893-904.

Dizhur, Dmytro, Jason Ingham, Lisa Moon, Mike Griffith, Arturo Schultz, Ilaria Senaldi, Guido Magenes et al, "Performance of masonry buildings and churches in the 22 February 2011 Christchurch earthquake", *Bulletin of the New Zealand Society For Earthquake Engineering*, Vol. 44, No. 4, December 2011, pp. 279-295.

Eiby, G. A., "An annotated list of New Zealand earthquakes, 1460–1965," *New Zealand Journal of Geology and Geophysics*, Vol. 11, No. 3, 1968, pp. 630-647.

Kaiser, A., C. Holden, J. Beavan, D. Beetham, R. Benites, A. Celentano, and D. Collett et al, "The Mw 6.2 Christchurch Earthquake of February 2011: Preliminary Report," *New Zealand Journal of Geology and Geophysics,* Vol. 55, No. 1, 2012, pp. 67-90.

Ministry of Civil Defence & Emergency Management. http://www.civildefence.govt.nz/memwebsite.nsf/wpg_URL/Media-Media-release-archive-Index?OpenDocument

Ministry of Civil Defence & Emergency Management. http://www.civildefence.govt.nz/

New Zealand Parliament, Canterbury Earthquake Recovery Act 2011. http://legislation.govt.nz/act/public/2011/0012/latest/DLM3653522.html?src=qs

New Zealand Tourism: http://www.newzealand.com/uk/christchurch/

New Zealand Tourism: http://www.newzealand.com/uk/christchurch-canterbury/

Pettinga, Jarg R., Mark D. Yetton, Russ J. Van Dissen, and Gaye Downes, Earthquake source identification and characterisation for the Canterbury region, South Island,

New Zealand *Bulletin of the New Zealand National Society for Earthquake Engineering*, Vol. 34, No. 4, 2001, pp. 282-317.

Reyners, Martin, Lessons from the destructive Mw 6.3 Christchurch, New Zealand, earthquake, *Seismological Research Letters,* Vol. 82, No. 3, 2011, pp. 371-372.

Statistics New Zealand, 2013 Census of Population and Dwellings.

TVNZ. http://tvnz.co.nz/national-news/christchurch-rebuild-balancing-act-cera-5846679

Cairns, Lois, "Housing pinch to worsen until 2017", *The Press,* 27 November 2013. http://www.stuff.co.nz/the-press/business/your-property/9446008/Housing-pinch-to-worsen-until-2017

University of Canterbury. http://www.ceismic.org.nz/

Whenmyhomeshook. http://whenmyhomeshook.co.nz/

3.3 STRESSING EVENTS THAT CONTINUE OVER A PERIOD OF TIME

This section covers the second type of adverse events – stressing events that continue over a period of time.

3.3.1 Resilience after the 2008 Global Financial Crisis

Professor Kirstie Ball, Open University

Introduction

Events surrounding the financial crisis of 2008 provide potentially significant insight into resilience-building in capitalist societies. They also reflect some problems with the concept of resilience and the protracted policy focus thereon. This short report will outline the findings of a literature review into issues of resilience surrounding the financial crisis. It will highlight the aspects of the financial system which need to be made more resilient in future. It also tackles the problem of path-dependency in society-level constructions of resilience as well as the elitism inherent in popular constructions of the concept. The report proceeds as follows. The first section outlines the sequence of events which prompted the financial crisis in 2008. It then examines the elements of the financial system which would need to be addressed in order for it to be made more resilient in future. Finally, it provides some critical reflections on the concept of resilience.

The Global Financial Crisis 2008

The Global Financial Crisis (GFC) of 2008 had its origins in the US and UK housing markets. Increases in house prices, excessive liquidity in financial markets coupled with the easy availability of credit led to a growth in mortgage lending, as sub-prime mortgages emerged in the USA and UK. Alongside the growth in sub-prime

mortgages came a deterioration in the risk controls surrounding lending, poor underwriting standards for sub-prime mortgages. This artificially inflated house prices, which triggered the financial crisis when home owners defaulted on their sub-prime mortgages en masse.

At the same time, in the financial markets, banks had repackaged these risky loans they had advanced to customers as 'asset backed securities' (ABS) which could be traded on capital markets. These were innovations, as far as financiers were concerned, and became significant in commercial and investment banking. They provided a source of finance for new loans and an avenue of investment for the banks, hedge funds, pension funds and other financial institutions.[497] Because ABSs were based on real estate and therefore had collateral, they were Triple A rated. However, they were so complex that the credit rating agencies themselves did not understand how they worked, and in some cases awarded the Triple A rating erroneously.

The defaults in sub-prime mortgages and the associated losses thus spread to the banks, hedge funds and other capital market investors. This destroyed demand for ABSs based on sub-prime mortgages in the financial markets. Banks and insurance companies that invested heavily in ABSs suffered huge losses and subsequently saw their share prices fall dramatically. The structure, operation and behaviour of traders within the financial markets accelerated the crisis exponentially.[498] It was demonstrated that traders showed 'herding' behaviour in times of stress, mimicking the behaviour of others, rather than evaluating situations for themselves.

The investment banks most heavily involved – such as Lehman Brothers - actually collapsed. In America three of the five large US investment banks had to be rescued or became insolvent, while the two Government-Sponsored Enterprises (GSEs) that specialised in structured finance, and the largest US insurance company, all had to be bailed out, at substantial cost to the US taxpayer. Figures from the European Commission show that between October 2007 and the end of 2011, European governments injected €440 billion ($605 billion) into their banks and provided guarantees of €1.1 trillion.[499] While all of Europe suffered economic recession, the economies of Greece, Italy and Spain were particularly hard hit because of the extent of credit-based finance in those countries.

Resilience following the financial crisis

Reflections on the financial crisis highlight a number of aspects of the global financial system which need to be made more resilient for the future. These areas relate to: macro-economic policy measures; institutional factors and the governance of institutions, and societal trust in financial institutions. Each of these factors will be considered in turn.

Macro-economic policy measures

[497] Tomasic, Roman, and Folarin, Akinbami, "The role of trust in maintaining the resilience of financial markets", *Journal of Corporate Law Studies*, Vol. 11, No. 2, pp. 369-394.
[498] Peron, Thomas Kaue Dal'Maso, Luciano da Fontoura Costa and Francisco A. Rodrigues, "The Structure and Resilience of Financial Market Networks", *Chaos* 22, 013117, 2012.
[499] The Economist, "From bail-out to bail-in", *The Economist*, 14 December 2013. http://www.economist.com/blogs/freeexchange/2013/12/european-banks

The resilience of different countries to the financial crisis has emerged as a topic for discussion. Many economists have attempted to explain, using macro-economic variables such as international trade and financial linkages,[500] how the crisis spread differentially between countries. Differing manufacturing demand,[501] vertical specialisation,[502] and credit conditions[503] played important roles. It was also established that foreign ownership of firms affected establishments' resilience to the GFC.[504] The subsidiaries of multinational corporations (MNC) were found to be more resilient and were able to sustain economic growth post-crisis. Thus, macro-economic policy measures which concern the encouragement of foreign direct investment (FDI) are also important. For many countries, such as Ireland, Slovakia, Singapore, and Malaysia, which have heavily relied on FDI for economic growth, there are increasing concerns that FDI is more volatile than domestic investments and causes greater economic vulnerability especially during economic crises. But different aspects of foreign ownership can exert sharply different, and even opposing, impact on establishment performance. For example, the ability of multinationals to shift production across countries can lead to more volatile performance while market diversification can lend stronger stability. It is the nature of the relationship between the parent organisation and the subsidiary which determines resilience.[505] Those subsidiaries which duplicate production activities of parent firms are more interchangeable and thus less resilient when financial difficulties arise. Those which are vertically integrated with the parent firms are mutually interdependent, not interchangeable and hence are more resilient. If demand drops away in the subsidiary host country, demand from the parent company will sustain that firms' financial performance.

Rather than focusing on the developed world, the International Monetary Fund (IMF) attempted to explain the differences in the crisis' impact across developing countries and emerging markets.[506] They found that countries in emerging markets with more leveraged (i.e. indebted) domestic financial systems and more rapid growth in lending to the private sector tended to suffer in terms of economic growth. For the rest, of the developing world, countries who exported advanced manufacturing goods were more affected than those exporting food. The demand for food was more resilient than the

[500] Rose, Andrew, and Mark Spiegel, "Cross-Country Causes and Consequences of the 2008 Crisis: International Linkages and American Exposure", *Pacific Economic Review,* Vol. 15, No. 3, 2010, pp. 340–63. Rose, Andrew, and Mark Spiegel, "Cross-Country Causes and Consequences of the 2008 Crisis: An Update", *European Economic Review,* Vol. 55, No. 3, 2011, pp. 309–24.
[501] Eaton, Jonathan, Sam Kortum, Brent Neiman, and John Romalis, "Trade and the Global Recession", 2009. http://economics.uchicago.edu/money_banking_papers/kortum111709.pdf
[502] Levchenko, Andrei A., Logan T. Lewis, and Linda L. Tesar, "The Collapse of International Trade during the 2008–09 Crisis: In Search of the Smoking Gun", *IMF Economic Review,* Vol. 58, No. 2, 2010, pp. 214–53.
[503] Chor, Davin, and Kalina Manova, "Off the Cliff and Back: Credit Conditions and International Trade during the Global Financial Crisis", Journal of International Economics, Vol. 87, 2012, pp. 117–133.
[504] Alfaro, Laura and Maggie Xiaoyang Chen, "Surviving the Global Financial Crisis: Foreign Ownership and Establishment Performance", *American Economic Journal: Economic Policy,* Vol. 4, No. 3, 2012, pp. 30–55.
[505] Ibid.
[506] Berkmen, Pelin, Gaston Gelos, Robert Rennhack, and James P Walsh, "The Global Financial Crisis: Explaining Cross-Country Differences in the Output Impact", *International Monetary Fund Working Paper* /09/280, 2009.

demand for manufacturing goods. Furthermore, those with flexible, rather than pegged exchange rates also dealt with the shock better. There was also some evidence that those with more robust government finances prior to the crisis were hit less severely, because they were able to deploy fiscal policy to counteract the crisis more effectively.

As a result of this work the IMF drew up some preliminary policy lessons for the developing world, focusing on macro-economic resilience:[507]

- Exchange-rate flexibility is crucial to dampen the impact of large shocks;
- Prudential regulation and supervision needs to aim at preventing the types of build up of vulnerabilities which are particularly associated with credit booms;
- A solid fiscal position during 'good times' creates some buffers to conduct countercyclical fiscal policies during shocks.

These issues also informed the OECD's response[508] in terms of its proposed resilient post-crisis macro-economic interventions. It goes as far as proposing greater covert macroeconomic surveillance and co-operative macroeconomic policy, but in a way which puts the financial linkages between countries, and their macro-economic policies under greater scrutiny. In particular, they emphasise the identification of risk and having greater powers to intervene in important economies which may be facing difficult times. This is similarly argued to be the case at the level of individual banks.[509] They argue that it is important to:

- Increase the focus on financial linkages between countries by strengthening multilateral surveillance of financial risk and the mutual assessment of macro economic policies of systemically important economies. This implies greater transparency and open-ness between countries at macro-economic level.
- Ensure that IMF and G20 risk identification processes focuses on external stability as a key metric – in order words, that they assess impact of high risk economic activities on surrounding and interconnected economies. Each country and currency area would need to indicate and then offer up for scrutiny a whole package of macro-economic policy measures. This would include greater exchange rate flexibility where needed.
- Pay due attention to financial imbalances and the macro-prudential dimension of oversight;
- Understand the root causes of poor macro-economic policy implementation rates and addressing them with appropriate instruments. These may include persuasion, external assistance, peer pressure, even-handedness, transparency, direct involvement of top officials, "comply or explain" procedures, greater independence and more inclusive governance of the IMF, as well as direct communication with – and enhanced accountability to – other countries.

---

[507] Dorrucci, Ettore, and Julie McKay, "The International Monetary System after the Financial Crisis", *IMF Occasional Paper Series* No. 123/February 2011. http://www.ecb.europa.eu/pub/pdf/scpops/ecbocp123.pdf

[508] Shigehara, Kumiharu, and Paul Atkinson, "Surveillance by International Institutions: Lessons from the Global Financial and Economic Crisis", *OECD Economics Department Working Papers*, No. 860, OECD Publishing, 2011.

[509] Bosworth, Ed and Tony Rich, "From optimisation to resilience:The changing nature of the risk reward conversation as seen through Westpac's capital and liquidity management policies", *Journal of Risk Management in Financial Institutions* Vol. 6, No. 2, 2012, pp. 160–166.

They also suggest that a global financial safety net be put in place, alongside financial market developments, to help emerging market and developing economies deal with external financial shocks, particularly those which result in sudden stops in capital inflows and losses of foreign currency. This financial safety net might also, provide an incentive to reduce the need for high accumulations of fiscal reserves to be used in a counter cyclical way.

Institutional factors and governance of institutions

From the previous section it is clear that the GFC prompted the overarching governance institutions such as the IMF, the European Central Bank and the OECD to issue a number of edicts about how macro-economic systems need to be strengthened and made more transparent in order to be resilient. It has also been suggested that the institutions themselves need better analytical tools and processes so they can respond to the surveillance agenda. A number of key problems with the current governance mechanisms within the institutions have been identified:

- While the recommendation is for effective surveillance of macro-economic policy on a number of technical issues, in the past such issues have been discussed at ministerial-level meetings at the IMF and the OECD. It is acknowledged that these are not suitable fora for technical policy discussions.
- The IMF executive board comprises 24 members residing in Washington who not directly involved in policy making and implementation in other capital cities around the world.
- At the OECD there has been an expansion of membership to 34 countries, and so the application of the peer pressure, identified as a 'soft power' measure in the previous section of this report, in order to ensure macro-economic open-ness and full policy implementation might be unevenly applied.
- Much of this work around macro-economic open-ness could be facilitated by the secretive Bank for International Settlements (BIS) committee, based in Basel. However while it is focused on financial co-operation between countries, is less geared up for surveillance of risk.

The OECD[510] itself has suggested that the IMF board and OECD committees relevant to surveillance may need to be restructured to ensure that enough pressure is placed on key countries and their central banks. For these key countries, it is suggested that bilateral surveillance should take place twice a year, less frequently for those who are less central to the global economy. An alertness to potential risks on these committees is called for and similar restructuring at the BIS is also required. The OECD also calls for greater co-operation between the IMF, OECD and BIS, if only on an informal level.

Developing internal organizational capacity in these institutions is an issue more generally. Dedicated, better qualified staff are required, who are capable of analysing the data and conducting the risk analyses required to identify problem areas. Previously, these institutions have been staffed by people seconded from national

[510] Ibid.

institutions, which presents problems in terms of succession planning, continuity and shared organisational knowledge. Inter departmental knowledge sharing is also considered an issue.

Finally, communication with stakeholders and the general public is something that these institutions feel they could improve upon. Enabling open data access to external analysts, speaking in non-obfuscatory language while not sanitising reports so as to gain the trust of stakeholders, are all seen as important. We focus more deeply on trust in the next section.

Trust in financial institutions

The final element of resilience following the GFC, trust, is a critical aspect which is not acknowledged by financial institutions, policymakers, or the macro-economists. The ability for any financial institution to attract customers, secure investment and subsequently drive economies forward after a crisis largely depends on the extent to which their stakeholders trust them to do what they say they will do. Trust is defined as "faith or confidence in the loyalty, strength, veracity... of a person or thing...without examination".[511] Tomasic and Folarin argue that the financial crisis resulted in a breakdown of trust between the banking sector and the rest of society which will take a long time to repair.[512]

When examining the issue of trust between financial institutions and society it is important to acknowledge that there are many intermediaries which sustain and produce that trust. Governing institutions, laws and regulations, the values, ethics of principles of the legal system inform notions of trust which underpin an individual's relationship with a bank. Emotions such as trust and confidence significantly influence the financial decision making of consumers[513]. Typically, consumers find it difficult to evaluate the risks associated with financial services products. They rely on regulations on the sale of these products to protect them in their decision making. It is argued that "the fragility of the financial system, built as it is on confidence, can mean that there is a real possibility of systemic risk spreading throughout the system".[514]

The erosion of confidence in the GFC was signified by, for example, the collapse of confidence in asset backed securities and the subsequent collapse in the financial markets. Another example is the collapse of confidence in key intermediaries, or gatekeepers, such as the credit ratings agencies. These agencies failed to assess the risks associated with ABSs adequately because they suffered from a conflict of interest.[515] The use of the innovative ABSs meant that ratings requests for these products were a large source of revenue for the agencies as they charged higher fees to rate them. Competition intensified in the ratings industry, when an additional ratings agency, Fitch, joined the existing duopoly of Standard and Poors and Moodys.

---

[511] Stevenson, A., *Shorter Oxford English Dictionary on Historical Principles*, Oxford University Press, Oxford, 2007.
[512] Tomasic and Folarin, op. cit., 2011.
[513] Gray, Joanna, and Jenny Hamilton, *Implementing Financial Regulation: Theory and Practice,* John Wiley, Chichester, 2006.
[514] Campbell, Andrew and Peter Cartwright, *Banks in Crisis: The Legal Response,* Ashgate Publishing, Aldershot, 2002, p. 7.
[515] Tomasic and Folarin, op. cit., 2011.

Rather than being faithful to their investors, they competed with each other. As it emerged that the credit ratings were flawed, many investors withdrew. Trust is crucial to enable the markets to operate smoothly. We now proceed to examine the current debate in perspective.

Resilience and the financial crisis in perspective

In the last section we identified the elements of the financial system which were considered important for increasing its resilience after the financial crisis. Macro-economic policy variables such as the degree of financial linkage between economies, exchange rate flexibility, fiscal reserves and foreign direct investment were identified as key areas of focus. Institutional surveillance of external risk and bilateral inspection of economic policies in key states were posited as the main interventions required, alongside organisational reform of the global financial governing bodies in order to make this happen. The building of trust and confidence in the financial system as a key resilient strategy was also covered both in terms of the effectiveness of laws and regulations governing the sale of financial products and the firm's individual behaviour towards its customers were important.

However, there have been other financial crises from which to learn, notably the Asian financial crisis of the late 1990s and the Turkish financial crisis of 2001. Examining what happened in these crises will enable us to establish that there is a degree of long term path dependency in the capacity of a nation or group of nations to be resilient to a financial crisis. Short term fixes are rooted with problems in long term strategies. The roots of Europe and the US's precipitation of, and response to this crisis will also lie deep in its mercantile and political history.

East Asian Financial Crisis 1997

The 1997 East Asian financial crisis stemmed from inappropriate borrowing by the private sector. Due to high rates of economic growth and a booming economy, private firms and corporations looked to finance speculative investment projects. However, firms overstretched themselves and a combination of factors caused a depreciation in the exchange rate as they struggled to meet the payments. The East Asian Economies of Thailand, Indonesia and South Korea had large current account deficits and total debt in the region was 167% of the GDP.

To examine resilience, we compare Malaysia, Thailand and Indonesia's reactions to the Asian financial crisis.[516] In the short term, Thailand adapted well to the shocks because out of the three countries it was the only democracy. It was thus more adaptable to external change than Malaysia and Indonesia which were authoritarian states and so were more resistant. Indonesia operated a harder authoritarian regime which suffered particularly badly in the financial crisis and has still not fully recovered. In the longer term, however, the picture has altered and indeed the regimes which are in place now are products of resilience in the face of that financial crisis. The Thai democracy broke down and is now unstable, having experienced a number of military coups in recent years. It is argued that Malaysia now has a more a hybrid

[516] Case, William, "after the Crisis: Capital and Regime Resilience in the ASEAN Three", *Journal of Contemporary Asia*, Vol. 39, No. 4, 2009, pp. 649-672.

system which is most resilient to financial shocks nowadays in that it retained its original hybrid form after the crisis. The explanation for this lies beyond the institutional ensemble and democratic procedures focused on in responses to the 2008 GFC, in the contingent patterns of capital ownership in these countries.[517] In Malaysia, ownership of capital was distributed between the state, indigenous and immigrant Chinese entrepreneurs and foreign direct investment. After the crisis it renationalised the assets of failed Malay businesses, preventing the loss of capital to overseas investors thus protecting the hybridity of the whole system, which still stands today. This current situation has deep historical roots in the way in which ethnic tensions were managed in the past.[518] Rather than divide and stigmatise overseas investors, historically the indigenous Malays co-opted Chinese investors in a hybrid political economy, who ultimately supported the state. In Indonesia and Thailand, where, for different reasons, entrepreneurs and investors were stigmatised and repressed, when the opportunity came following the crisis they effectively competed with each other and 'looted' state resources, damaging the whole economy in the long term. Ironically one of the IMFs recommendations following the 1997 crisis was that Asia liberalise their economies, remove restrictions on foreign ownership and to state-business relations that would make them more like their Western counterparts.[519] However, it was unique aspects of their national history that worked to make them more resilient when their Western counterparts crashed in 2008.

Having lived through one financial crisis in the late 1990s, many East Asian countries were then better equipped to deal with the GFC.[520] They have not been completely immune, as they have experienced contractions in GDP and export growth rates in 2008 – 2009, as well as foreign currency liquidity shortages. However, these impacts did not last long, and by 2010 they had returned to their pre-crisis economic performance levels. Employment levels, industrial capacity utilisation, domestic investment and business confidence had each returned to normal.[521] In fact, these East Asian economies were seen to be leading (for the first time) a global recovery.[522] Because of their policy responses to the 1997 crisis, East Asian countries in general had lower levels of debt and higher central bank reserves – things that have been recommended to Western countries in the GFC 2008.[523] They also understood the need to respond quickly to the onset of a crisis, adjusted their currencies and provided large stimulation packages rapidly. This is not to suggest that there are not still significant weakness in these economics. However, they have addressed some of the risks and are judged to have the resources, capacity and confidence to face future crises, more so than elsewhere in the global economic system.

---

[517] Ibid.
[518] Ibid.
[519] Bullard, Nicola, "Taming the IMF: How the Asian crisis cracked the Washington Consensus", in P. Masina, (ed.), *Rethinking development in East Asia: From illusory miracle to economic crisis,* Curzon, Richmond, 2002, pp. 144-160.
[520] Dixon, Chris, "The Roots of East Asian Resilience to the Financial Crisis", *Journal of Asia Pacific Studies,* Vol. 2, No. 3, 2012, pp. 374 – 388.
[521] World Bank, *Robust recovery, rising risks. East Asia and Pacific Economic Update 2010,* Volume 2, World Bank, Washington, 2010.
[522] World Bank, *Securing the present, shaping the future. East Asia and Pacific Economic Update 2011*, Volume 1, World Bank, Washington, 2011; IMF, *Regional economic outlook: Asia and Pacific leading the global recovery rebalancing for the medium term*, IMF, Washington, 2010.
[523] World Bank, East Asia and Pacific Economic Update, 2008. http://eapblog.worldbank.org/month/2008/12

Turkish financial crisis 2001

There is a similar story in relation to Turkey, which had its own financial crisis in 2001 after ten years of deep and long recessions. The recent global financial crisis of 2008, however, was a turning point in Turkey's economic development. During this crisis, the Turkish economy stayed resilient to the economic downturn. It was observed that although the country's GDP suffered to a greater extent than other emerging economies, it bounced back much faster and much more strongly.[524] Some of the main financial indicators, discussed earlier in this report were affected less badly:

- Capital outflows: Short term and long term private external debt decreased, but not to the same extent as in earlier crises (3% in 2008 when compared to 6% in 2001)
- Foreign currency credit availability (prevents home currency from depreciating): in 2001, Turkish Lira and Dollar credits both decreased by 40%, whereas in 2008 they decreased by 5% and 20% respectively.
- Credit to GDP ratio (a measure of national creditworthiness): in 2001 this decreased from 29% - 16%; in 2008 it only decreased from 46% - 44%. As a result domestic credit markets did not contract during 2008.

The main reason for the resilience of Turkey's economy was the strong fiscal stance taken by the Turkish government after 2001. Following that crisis, the government had built up significant financial reserves, which enabled the Central Bank of the Republic of Turkey to circulate enough liquid assets in the economy (termed quantitative easing) in 2008 which enabled it to continue functioning. Interest rates and taxes were also cut in 2008. The overall picture of financial health at a government level discouraged firm owners from being tempted to transfer their financial wealth abroad, as they placed their trust in the Turkish economy. Finally because financial wealth in the general population was already quite low, there were little perceived or actual losses as a result of the crisis.

Viewing the financial crisis in perspective, it is clear that technical economic, monetary and fiscal measures do play a part in ensuring resilience in financial crises. However, prudence, learning from past experience, and historical politico-economic and community factors also have a role to play.

Critiquing resilience

On reviewing the evidence it appears that financial resilience can be fostered in technical, institutional, politico-economic and social settings, and there are many lessons to be learned from around the world. However, according to critical commentators Raco and Street (2012),[525] policy discourses about resilience following

[524] Kılınç, Mustafa, Zübeyir Kılınç and M. Ibrahim Turhan, "Resilience of the Turkish Economy During the Global Financial Crisis of 2008", *Emerging Markets Finance & Trade,* November–December 2012, Vol. 48, Supplement 5, pp. 19–34.

[525] Raco, Mike and Emma Street, Resilience Planning, Economic Change and The Politics of Post-recession Development in London and Hong Kong Urban Studies, Vol. 49, No. 5, 2012, pp. 1065 – 1087.

the GFC 2008 seem to be very context-specific and formulated within a narrow field of reference. They argue that resilience planning has become path-dependent, and that these path dependencies are shaped by past experience within that particular context as well as earlier policy successes and failures. Wider frames of reference, such as the experiences of East Asia or Turkey, are rarely taken into account. The focus resolutely seems to be on the issues of recovery from stresses and shocks at the level of elites and their respective interests.[526] Everyone else seemingly just has to adapt to external changes. After examining post-recession planning in both Hong Kong and London, they also critique resilience discourses as being inherently conservative, focusing on 'more of the same' rather than anything genuinely innovative or developmental. This stems from the tendency of resilience to be concerned with preservation of the *a priori* status quo and having a focus on the past. Given that it was what happened in the past that provoked the crisis, it is questionable whether a return to that past is actually desirable.

New forms of democratic participation in a range of non-market institutions are needed to critique the power of these financial elites, and to move away from the conservatism inherent in the concept of resilience.[527] Engelen et al argue that the social function of high finance needs to be brought into the debate.[528] Within the city of London, there is a weak history of democratic engagement with (i.e. the regulation of) financial elites which almost certainly contributed to the current state of affairs. Powerful financial institutions were allowed to operate 'at arms' length' from the government which had disastrous results for society as a whole. With the decline in Trade Unionism in the UK, traditional bastions of democratic scrutiny and challenge, and a rebranding of the traditional left giving way to 'new labour', the traditional routes of democratic participation closed down. Engelen et al argue:

> there is a *substantive* [original emphasis] agenda for reform of the financial system…But that substantive agenda has no hope of being realized if it is promoted through the established institutional world of political, regulatory and financial market elites. Any alternative must engage with the opportunities created by the new worlds of popular mobilization and engagement…[529]

Hostility to the irresponsibility of financial institutions, they argue, needs to be challenged by highlighting how they delivered the wrong kind of financial system for all in society. And then focus needs to be placed on how finance could serve unmet social needs in future. Social media, the NGOs and existing trade union networks could be mobilised to this effect, and this would represent innovative resilience in response to the GFC of 2008.

Conclusion

In the GFC 2008, easy monetary policies led to the accumulation of large amounts of foreign exchange reserves, which subsequently caused global imbalances. These imbalances were caused by "...flaws in the design and implementation of

---

[526] Ibid.

[527] Engelen, E., et al, *After the Great Complacence: Financial Crisis and the Politics of Reform*, Oxford University Press, Oxford, 2011.

[528] Ibid.

[529] Engelen, op. cit., 2011, p. 243.

macroeconomic policies around the world and by the resulting global credit boom".[530] Financial excess was manifested by housing booms in the USA and other countries and by increased prices of equities. The fact that financial innovations, such as ABSs, were not well understood led to an underestimation of risks associated with them by the credit rating agencies. At the centre of the financial crisis were the large, privately-owned, financial institutions, which became overextended and in the end failed due to their size and complexity. The failures in macroeconomic policies and in the existing financial-sector supervision and regulation were hence the main causes of the recent global financial crisis.

In conclusion, a number of aspects of the financial system need to be amended in order to avoid future crises and to make economies more financially resilient in the future. These aspects were:

- Macroeconomic policies
- Financial-sector supervision and regulatory policies
- Public trust in the financial system

However, drawing on the experience of the East Asian countries in particular, it pays to strengthen the nature of democratic interaction with the financial world, take lessons from history, and genuinely break with the past to avoid similar problems in future.

References

Alfaro, Laura and Maggie Xiaoyang Chen, "Surviving the Global Financial Crisis: An Update", *European Economic Review,* Vol. 55, No. 3, 2012, pp. 309–324.

Berkmen, Pelin, Gaston Gelos, Robert Rennhack, and James P. Walsh, "The Global Financial Crisis: Explaining Cross-Country Differences in the Output Impact", *International Monetary Fund Working Paper* /09/280, 2009.

Bosworth, Ed, and Tony Rich, "From optimisation to resilience:The changing nature of the risk reward conversation as seen through Westpac's capital and liquidity management policies", *Journal of Risk Management in Financial Institutions* Vol. 6, No. 2, 2012, pp. 160–166.

Bullard, Nicola, "Taming the IMF: How the Asian crisis cracked the Washington Consensus", in P. Masina, (ed.), *Rethinking development in East Asia: From illusory miracle to economic crisis,* Curzon, Richmond, 2002, pp. 144-160.

Campbell, Andrew and Peter Cartwright, *Banks in Crisis: The Legal Response,* Ashgate Publishing, Aldershot, 2002.

Case, William, "after the Crisis: Capital and Regime Resilience in the ASEAN Three", *Journal of Contemporary Asia*, Vol. 39, No. 4, 2009, pp. 649-672.

[530] Truman, Edwin M., "Lessons from the Global Economic and Financial Crisis," Keynote address at the conference ―G-20 Reform Initiatives: Implications for the Future of Regulation, Seoul, Korea, 11 November 2009. http://www.iie.com/publications/papers/truman0911.pdf

Chor, Davin, and Kalina Manova, "Off the Cliff and Back: Credit Conditions and International Trade during the Global Financial Crisis", Journal of International Economics, Vol. 87, 2012, pp. 117–133.

Dorrucci, Ettore, and Julie McKay, "The International Monetary System after the Financial Crisis", *IMF Occasional Paper Series* No. 123/February 2011. http://www.ecb.europa.eu/pub/pdf/scpops/ecbocp123.pdf

Dixon, Chris, "The Roots of East Asian Resilience to the Financial Crisis", *Journal of Asia Pacific Studies,* Vol. 2, No. 3, 2012, pp. 374 – 388.

Eaton, Jonathan, Sam Kortum, Brent Neiman, and John Romalis, "Trade and the Global Recession", 2009.
http://economics.uchicago.edu/money_banking_papers/kortum111709.pdf

Engelen, E., et al, *After the Great Complacence: Financial Crisis and the Politics of Reform*, Oxford University Press, Oxford, 2011.

Gray, Joanna, and Jenny Hamilton, *Implementing Financial Regulation: Theory and Practice,* John Wiley, Chichester, 2006.

IMF, *Regional economic outlook: Asia and Pacific leading the global recovery rebalancing for the medium term*, IMF, Washington, 2010.

Kılınç, Mustafa, Zübeyir Kılınç and M. Ibrahim Turhan, "Resilience of the Turkish Economy During the Global Financial Crisis of 2008", *Emerging Markets Finance & Trade,* November–December 2012, Vol. 48, Supplement 5, pp. 19–34.

Levchenko, Andrei A., Logan T. Lewis, and Linda L. Tesar, "The Collapse of International Trade during the 2008–09 Crisis: In Search of the Smoking Gun", *IMF Economic Review,* Vol. 58, No. 2, 2010, pp. 214–53.

Peron, Thomas Kaue Dal'Maso, Luciano da Fontoura Costa and Francisco A. Rodrigues, "The Structure and Resilience of Financial Market Networks", *Chaos* 22, 013117, 2012.

Raco, Mike and Emma Street, Resilience Planning, Economic Change and The Politics of Post-recession Development in London and Hong Kong Urban Studies, Vol. 49, No. 5, 2012, pp. 1065 – 1087.

Rose, Andrew, and Mark Spiegel, "Cross-Country Causes and Consequences of the 2008 Crisis: International Linkages and American Exposure", *Pacific Economic Review,* Vol. 15, No. 3, 2010, pp. 340–63.

Rose, Andrew, and Mark Spiegel, "Cross-Country Causes and Consequences of the 2008 Crisis: An Update", *European Economic Review,* Vol. 55, No. 3, 2011, pp. 309–24.

Shigehara, Kumiharu, and Paul Atkinson, "Surveillance by International Institutions: Lessons from the Global Financial and Economic Crisis", *OECD Economics Department Working Papers*, No. 860, OECD Publishing, 2011.

The Economist, "From bail-out to bail-in", *The Economist*, 14 December 2013. http://www.economist.com/blogs/freeexchange/2013/12/european-banks

Tomasic, Roman, and Folarin, Akinbami, "The role of trust in maintaining the resilience of financial markets", *Journal of Corporate Law Studies*, Vol. 11, No. 2, pp. 369-394.

Truman, Edwin M., "Lessons from the Global Economic and Financial Crisis," Keynote address at the conference ―G-20 Reform Initiatives: Implications for the Future of Regulation, Seoul, Korea, 11 November 2009. http://www.iie.com/publications/papers/truman0911.pdf

World Bank, East Asia and Pacific Economic Update, 2008. http://eapblog.worldbank.org/month/2008/12

World Bank, *Robust recovery, rising risks. East Asia and Pacific Economic Update 2010,* Volume 2, World Bank, Washington, 2010.

World Bank, *Securing the present, shaping the future. East Asia and Pacific Economic Update 2011*, Volume 1, World Bank, Washington, 2011

3.3.2 Google Street View collection of payload data

Dr Rowena Rodrigues, Trilateral Research & Consulting

Nature of the adverse event

Google Street View is a Google Maps application used to explore places through 360-degree street-level imagery from public spaces and privately owned properties (that have permitted such access).[531] Google collects this imagery through its vehicles driving past locations, processes it and subsequently puts it online.

Google's Street View prompted privacy and security concerns when it collected payload information from Wi-Fi connections in an unauthorised manner in a number of countries.[532] Data collected included entire e-mails, URLs and passwords. Several countries launched investigations – Australia, Austria, Belgium, Canada, France, Germany, Greece, Hong Kong, Irish Republic, Italy, New Zealand, Switzerland, the UK and the US.[533] In the UK, news of the Google Street View collection of payload data emerged in May 2010.

[531] Google Inc., "Using Street View". http://maps.google.co.nz/intl/en/help/maps/streetview/learn/using-street-view.html

[532] Arthur, Charles, "Google's problem is that it now believes itself above others – even governments", *The Guardian,* 1 May 2012. http://www.guardian.co.uk/technology/2012/may/01/google-street-view-data-fcc

[533] See Electronic Privacy Information Centre (EPIC), "Investigations of Google Street View". http://epic.org/privacy/streetview/

We characterise the unauthorised collection of payload data as an adverse event worthy of analysis for the following reasons: first, it broadly represented a threat in terms of privacy, personal data protection rights, its potential to chill and monitor individuals' behaviour, speech and expression, and affect personal autonomy and reputation. Second, the incident affected a large number of countries and people. Third, it concerned a key industry player that controls a large swath of the Internet and has a huge capacity to monitor communications on it – this is a good example of privatised surveillance function creep. Fourth, this incident affected the public and institutional perception of Google adversely, particularly in Europe.

Institutional response

The UK Information Commissioner's Officer (ICO) asked Google for details of Street View's operations and assurances in relation to data it collected after Google was criticised by the German Federal Commissioner for Data Protection.[534] The ICO visited Google's premises to assess the payload data samples, and acknowledged that it was wrong for Google to collect the information; however, the ICO was "satisfied so far that it is unlikely that Google will have captured significant amounts of personal data. There is also no evidence as yet that the data captured by Google has caused or could cause any individual detriment."[535] The media severely criticised by the ICO's stance as being too soft on Google.[536]

The Metropolitan police investigated a complaint by Privacy International which alleged that that Google's capture of Wi-Fi data breached the Regulation of Investigatory Powers Act 2000 (RIPA).[537] After consulting with the ICO, the Metropolitan police decided "it would not be appropriate to launch a criminal investigation".[538]

In October 2010, the ICO reopened the Google Street View investigation after Google publicly acknowledged that though most of the data it had captured was fragmentary, in some instances it included entire e-mails, URLs and passwords.[539]

A motion tabled in the UK House of Commons on 25 October 2010 noted that "the Information Commissioner had previously failed to take substantial action, despite the example set by most countries in Europe, Canada, South Korea and others" and called upon the ICO "to take a robust approach" that would protect individual freedom from

---

[534] Williams, Christopher, "UK data watchdog to quiz Google on Streetview Wi-Fi database", *The Register,* 26 April 2010. http://www.theregister.co.uk/2010/04/26/google_wifi_ico/

[535] Information Commissioner's Office (ICO), "Google – Assessment of Wi-Fi data", Statement, 29 July 2010.

[536] Williams, Christopher, "ICO defends soft Street View probe, insists case still open", *The Register,* 12 August 2010. http://www.theregister.co.uk/2010/08/12/ico_google/

[537] BBC News, "Google under investigation by Met police", *BBC News*, 23 June 2010. http://www.bbc.co.uk/news/10391096

[538] Mitchell, Stewart, "Police drop probe into Google Street View fiasco", *PC Pro,* 29 October 2010. http://www.pcpro.co.uk/news/362386/police-drop-probe-into-google-street-view-fiasco

[539] Eustace, Alan, "Creating stronger privacy controls inside Google", *Google official blog*, 22 October 2010. http://googleblog.blogspot.in/2010/10/creating-stronger-privacy-controls.html

the "threat of a privatised surveillance society".[540] Another motion tabled on the same date stated,

> That this House is deeply concerned at the statement of Alan Eustace, senior vice-president for engineering and research at Google, when he admitted that his company's Street View cars captured entire e-mails and URLs... as well as passwords; notes that Google has promised to make changes to internal compliance procedures; also notes, however, that in recent months there has been a series of invasions of personal privacy by the firm, which are beginning to look like a pattern; therefore welcomes the Backbench Business Committee debate into these matters on 28 October 2010; and calls on the Information Commissioner to be thorough and proactive in its inquiry.[541]

In November 2010, the ICO concluded that there had been a significant breach of the Data Protection Act 1998 when Google Street View cars collected payload data as part of their Wi-Fi mapping exercise in the UK.[542] Google signed an undertaking in November 2010 confirming the steps it would take to ensure personal data was processed in accordance with the first principle in Part 1 of Schedule 1 to the Data Protection Act 1998. Google also agreed to facilitate a consensual audit within nine months from the date of the undertaking. The audit conducted in July 2011 reviewed the confidential Privacy Report provided by Google to the ICO. According to the ICO, the audit "provided reasonable assurance over the accuracy and findings of the Privacy Report as provided by Google Inc. to the Information Commissioner" and "reasonable assurance that Google have implemented the privacy process changes outlined in the Undertaking".[543] The audit identified some areas of improvement.

In April 2012, the US Federal Communications Commission (FCC) concluded its investigation into Google's capture of payload data across the USA and concluded that Street View cars had for over two years "collected names, addresses, telephone numbers, URLs, passwords, e-mail, text messages, medical records, video and audio files, and other information from Internet users in the United States".[544] The ICO reviewed the FCC findings and concluded "it seemed likely that such information was deliberately captured during the GSV operations conducted in the UK",[545] as opposed

---

[540] Halfon, Robert (primary sponsor), "Information Commissioner and internet privacy", Early Day Motion 882, Session 2010-12, 25 October 2010. http://www.parliament.uk/edm/2010-12/882

[541] Halfon, Robert (primary sponsor), "Google and the capture of data using Street View cars", Early Day Motion 883, Session 2010-12, 25 October 2010. http://www.parliament.uk/edm/2010-12/883

[542] ICO, "Information Commissioner announces outcome of Google Street View investigation", *Press release,* 3 November 2010.
http://www.ico.org.uk/~/media/documents/pressreleases/2010/google_inc_street_view_press_release_03112010.pdf

[543] ICO, "Google Inc. Data Protection Audit Report", *Executive Summary*, August 2011.
http://ico.org.uk/news/latest_news/2011/~/media/documents/library/Data_Protection/Notices/ico_audit_google_executive_summary.ashx

[544] Federal Communications Commission (FCC), *In the matter of Google Inc. before the FCC,* DA 12-592, 13 April 2012. The FCC did not find the collection to be per se unlawful and decided not to take any enforcement action against Google in relation to the same. However, the FCC fined Google $25,000 for wilfully and repeatedly violating the Enforcement Bureau directive to respond to a letter of inquiry (i.e., Google had failed to: provide compliant declarations verifying completeness and accuracy of its letter of inquiry responses for nearly nine months; identify Google employees with knowledge of relevant facts and search for and produce any e-mails.

[545] ICO, Letter to Google Inc., 11 June 2012.

to the 2010 situation where the ICO had been "specifically told by Google that it was a simple mistake".[546] The ICO asked Google to: precisely list the type of personal and sensitive personal data that formed part of the payload data collected in the UK; confirm the point at which Google managers became aware of the type of payload data captured during UK operations and the type of technological and organisational measures introduced to limit further collection prior to Google's admission of 14 May 2010; provide a substantial explanation of why this type of data was not included in the pre-prepared data sample presented to the ICO; advise of the point at which senior Google managers had seen the software design documents, been briefed of the code and the type of data it could capture; provide copies of the original software design document and associated logs; outline privacy concerns identified by Google and threat management on revelation of the practice; and finally, outline the measures introduced to prevent breaches of the Data Protection Act 1998 at each stage of the Google Street View process.[547]

In its reply to the ICO, Google expressed surprise at the re-opening of the investigation.[548] Google clarified, inter alia, that it had not pre-prepared data for the inspection and that it could not "definitively list what types of personal data and/or sensitive personal data were captured within the payload collected in the UK".[549] Google also commented that the publication of the FCC's findings did "not in any way change the position from that at the time that Google and the ICO agreed Undertakings in November 2010".[550] Soon after this, on 27 July 2012, Google informed the ICO (after a review of Street View disks) that it still possessed a small portion of payload data collected by Street View vehicles in the UK, apologised for its error, and said that it would co-operate in deleting the rest of the UK data.[551]

So what can we conclude about the institutional response to the Street View collection of payload data in the UK? The institutional response at best can be said to be fractured, reactive and not at all geared to effectively address threats to society and its values based on frameworks that exist. The ICO deputy commissioner David Smith himself acknowledged, "Look at Google with the payload data they take from Street View. We didn't do a very good job there", and that "Some of our colleagues have found Street View unacceptable, but we think banning Street View because of privacy invasion would be a step too far and not what our citizens want. Other nation's citizens may feel differently."[552]

---

http://www.ico.org.uk/~/media/documents/library/Corporate/Notices/google_letter_alan_eustace_20120611.ashx

[546] Ibid.

[547] Ibid.

[548] Fleischer, Peter, "Google Street View Wi-Fi Collection", Letter to ICO, 18 June 2012.

[549] Ibid. See also Essers, Loek, "Google 'surprised' by revived UK Street View investigation", *Computerworld,* 20 June 2012. http://www.computerworld.com/s/article/print/9228281/Google_surprised_by_revived_UK_Street_View_inves

[550] Fleischer, Peter, "Google Street View Wi-Fi Collection", Letter to ICO, 18 June 2012.

[551] Fleischer, Peter, "Google Street View Wi-Fi Collection", Letter to ICO, 27 July 2012 http://www.ico.org.uk/news/current_topics/~/media/documents/library/Corporate/Notices/20122707_letter_Google_to_ICO.ashx

[552] Stevenson, Alastair, "Right to be forgotten on the web unworkable, argue data watchdogs", *V3.co.uk*, 26 March 2013. http://www.v3.co.uk/v3-uk/news/2257523/right-to-be-forgotten-unworkable-argue-data-watchdogs

Economic response

It is difficult to assess the economic response to the collection of payload data by Google Street View.

One company issued a technical note on the lessons to be learnt from the Google Street View incident. Based on the FCC decision, it provided the following advice for wireless local area network (LAN) planners, administrators and enthusiasts who routinely discover nearby networks:

1. First, this case focused on data payload. Beacons, probe responses, and other headers commonly used for WLAN analysis do not seem to have posed concern. Lesson: We can be comfortable recording these frames during WLAN discovery.
2. Second, although the Act allows interception of electronic communication readily accessible to the general public, the investigation was triggered by data payload recording. Lesson: If payload is not necessary, don't record it.
3. Third, WLAN owners can consent to recording their own traffic, but Street View recorded traffic from other WLANs. Furthermore, what was done with that data played a big role. If encrypted data had been cracked, the ruling could have differed. Lesson: If you plan to drill into data, get permission first.
4. Finally, every WLAN professional should understand what data their tools record so that it can be treated appropriately. This just might be the biggest lesson of all.[553]

Thus, the incident clarified to a certain extent what may and may not be acceptable practice for other companies indulging or seeking to indulge in related activities.

Societal response

Civil society organisations in the UK (and elsewhere) censured Google's collection of payload data in the media. They criticised the ICO's response to the incident very sharply.[554] For instance, Alex Deane, director of Big Brother Watch (a UK-based privacy and civil liberties campaign group) commented, "The information commissioner's failure to take action is disgraceful. Ruling that Google has broken the law, but then taking no action against it, shows the commissioner to be a paper tiger."[555] In 2012, Big Brother Watch welcomed the re-opening of the investigation into Google; it believed that the 2010 ICO investigation lacked vigour and called for a "thorough investigation and an outcome that sets a firm precedent going forward that companies – however big – should respect the privacy of UK citizens and that 'deliberate accidents' will not be tolerated".[556] EPIC (a US-based public interest non-profit research group) has an observatory on investigations of Google Street View.[557]

---

[553] Phifer, Lisa, "What We Can Learn from Google Street View," A TechNote on Wireless and Mobility, *Webtorials,* May 2012. http://www.webtorials.com/content/2012/05/what-we-can-learn-from-google-street-view.html

[554] Petrou, Andrea, "ICO sent unqualified staff to investigate Google", *TechEYE.net,* 10 Nov 2010. http://news.techeye.net/security/ico-sent-unqualified-staff-to-investigate-google

[555] Halliday, Josh, "Google committed 'significant breach' over Street View", *The Guardian,* 3 Nov 2010.
http://www.guardian.co.uk/technology/2010/nov/03/google-information-commissioner-street-view

[556] Big Brother Watch, "ICO reopens Google Spy-Fi investigation", 12 June 2012.
http://www.bigbrotherwatch.org.uk/online-privacy/page/4

[557] EPIC, "Investigations of Google Street View". http//epic.org/privacy/streetview/

The media projected Google's collection of payload data in the UK in a number of ways: cautionary, expressing outrage, chastising. One headline projected Google had been accused of criminal intent (based on views expressed by Privacy International).[558]

The *Daily Mail*'s David Thomas was reportedly out to take his "own small stand against the Google monster", the information "stolen" through use of the Street View cars and stored, whether it had been destroyed and what data had been retained.[559] Thomas criticised the ICO and questioned why "neither the ICO, nor anyone else" questioned Google about "why they needed to have any data-capturing software on their Street View cars at all".[560] Thomas requested readers of the *Daily Mail* to join his campaign against Google.

The Google Street View payload data collection incident arguably created and reinforced a broader general public awareness of privacy and data protection and a more specific sense of awareness of the dangers of exposing personal and sensitive personal data over Wi-Fi (particularly unsecured Wi-Fi) networks.[561] To some extent, we could say that this prompted an increase in the use of encryption to protect privacy and personal data and reduction in or more cautionary use of public unsecured Wi-Fi networks.

The negative press in relation to the collection, retention, failure to destroy payload data and Google's misleading positions in the matter has affected Google's public image. The incident caused a certain increase in the mistrust of Google, its practices and its potential to address privacy and data protection harms (the extent of this, however, is not clear, in the absence of a specific study to that effect). The scepticism about Google's motives is also illustrated by one headline that termed the unauthorised collection as "an intentional mistake".[562] However, another comment states

> Google's interception of so-called 'private' data broadcast over unencrypted residential wireless networks could have, and probably has been done by many other companies, and that it has come to light that Google has, should be a wake-up call to people to encrypt private information, not a reason to, strictly-speaking, hate Google.[563]

---

[558] BBC News, "Google accused of criminal intent over Street View data," *BBC News,* 9 June 2010. http://www.bbc.co.uk/news/10278068

[559] Thomas, David, "Why I'm going into battle with Google to find out if it stole my family's secrets", *Daily Mail Online,* 13 June 2012. http://www.dailymail.co.uk/debate/article-2158992/Why-I-m-going-battle-Google-stole-family-s-secrets.html#ixzz2QgnYgND7

[560] Ibid.

[561] For example, see comments by Thomas, op. cit., 2012. Such comments are echoed in Kravets, David, "An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle", *Wired,* 5 February 2012. http://www.wired.com/threatlevel/2012/05/google-wifi-fcc-investigation/. Commentators went so far as to suggest that that "if you have an unencrypted wi-fi broadcasting publicly you deserve everything you get" or "why anyone has any expectation of privacy with data transmitted over an unencrypted Wireless LAN. If you want privacy, configure encryption."

[562] Kravets, ibid.

[563] West, Benjamin, "Comment" in David Kravets, "An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle", *Wired,* 5 February 2012. http://www.wired.com/threatlevel/2012/05/google-wifi-fcc-investigation/

Thus, it might be questionable whether Google's reputation has been significantly or substantially harmed by its collection of payload data. This is particularly concerning as it sets a dangerous precedent for other companies.

Conclusions

In Google's collection of payload data in the UK, we see an overall relative inability to deal with this incident. Legislation, despite its establishment and general prevalence (e.g., the EU Data Protection Directive of 1995, the UK Data Protection Act 1998) failed to guard against the incident and does not seem to have prevented the company from breaching privacy and data protection rights. The regulator (in this instance, the ICO) failed to deal with the incident appropriately – attributable either to a good faith belief in the company or a lack of time, technical and human resources. Google, free to operate in an environment of self-regulation, failed to evaluate its technology for threats (no privacy impact assessment of Street View was conducted before its launch), take mitigation measures, and address consequences effectively.[564] The UK ICO failed to hold Google to account (in comparison to actions by other regulators – the French CNIL fined the company €100,000 in 2011,[565] the US got Google to agree to pay a fine of $7 million in 2013,[566] and the German data protection authority fined Google €145,000 in 2013).[567] This shows that while the threats and potential harms caused by the Street View's capture were nearly the same in the different countries, the UK approach in dealing with the incident seems to have been comparatively feeble.

A certain laissez-faire attitude is evident on the part of society and individuals in the UK to the threat from Google's unauthorised collection, retention and casual attitude to destroying payload data (given the lack of public opposition compared to other surveillance threats). What is perturbing is that individuals displayed a certain sense of acceptance of surveillance of personal data put at risk (intentional or otherwise) through lack of use of security measures, i.e. , individuals seem less troubled about surveillance of personal data that is not adequately protected by personal data subjects. Even civil society organisations treated this event on a lesser priority basis.

What lessons might be learnt from this experience?

---

[564] Google hired security consulting firm Stroz Friedberg to evaluate the Street View software. Stroz Friedberg, "Source Code Analysis of gstumbler", prepared for Google and Perkins Coie, 3 June 2010. http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf; Google conducted privacy impact assessments for Street View in Australia and New Zealand, but that was at the behest of the NZ Privacy Commissioner. Google, "Google Street View Australia Privacy Impact Assessment", April 2011. http://services.google.com/fh/files/blogs/google_streetviewaustraliaprivacyimpactassessment.pdf; Google, "Google Street View New Zealand Privacy Impact Assessment", August 2011. http://services.google.com/fh/files/blogs/New%20Zealand%20Street%20View%20Privacy%20Impact%20Assessment%20August%202011.pdf

[565] Commission nationale de l'Informatique et des Libertés (CNIL), "Google Street View: CNIL pronounces a fine of 100,000 Euros", *CNIL News,* 21 March 2011. http://www.cnil.fr/english/news-and-events/news/article/google-street-view-cnil-pronounces-a-fine-of-100000-euros/

[566] BBC News, "Google hit by $7m Street View fine in US", 12 March 2013. http://www.bbc.co.uk/news/technology-21762545

[567] BBC News, "Google fined over illegal wi-fi data capture in Germany", 22 April 2013. http://www.bbc.co.uk/news/technology-22252506

First, there is a need for a more proactive and efficient approach to regulate privatised surveillance and its effects.

Second, there is a need to inculcate and develop a culture of vigilance to surveillance, particularly in relation to the design and implementation of new technologies. This vigilance is a multi-dimensional construct, needing to be developed by each stakeholder and across stakeholders. Shared vigilance is more powerful than individual vigilance (which might be of limited effect due to individual motivations).

Third, the collection of payload data occurred in different countries; different countries in the EU dealt with the problem differently; some seemingly more effectively and others less so. We recommend better co-ordination, sharing of information and learning of lessons between relevant authorities across the EU.

Fourth, is the need for greater accountability, particularly on the part of industrial actors designing and implementing cutting edge surveillance solutions without adequate investment in examining effects or monitoring threats from those solutions that affect or have the potential to affect human rights and fundamental freedoms. The incident clearly shows the failure of a self-regulatory regime for privacy and data protection.

3.3.3 UK National DNA Database and the case of S v. Marper

Dr Rowena Rodrigues, Trilateral Research & Consulting

The England and Wales National DNA database (NDNAD), administered by the National Policing Improvement Agency (NPIA) and governed by the NDNAD Strategy Board[568], is the largest forensic database in the world. Reports suggest the database has five million DNA profiles stored and "is the largest per capita DNA database in the world, second in size only to the USA"[569]). In 2001, an amendment to the law permitted DNA samples and fingerprints to be retained indefinitely.[570] Any individual arrested for a recordable offence in England, Wales and Northern Ireland could have their DNA sample taken and stored as profiles on the national DNA database. It did not matter if the individual was never charged, the criminal proceedings were discontinued or the individual was acquitted of the crime.

The unlimited collection of DNA samples and retention of profiles by police in England, Wales and Northern Ireland on the NDNAD may not strictly be regarded as an "adverse event" as compared to other events analysed in this report; however, it satisfies the "adversity" requirement for the following reasons: its potential to threaten privacy and personal life, threat to other civil liberties, scope for misuse and function

[568] As of 1 December 2012, the NPIA ceased operations. Some of its functions were transferred to the College of Policing and others were transferred to the Home Office. Administration of the Police National Computer (PNC), of which the Police National Database (PND) is a part, was transferred to the Home Office.
[569] Liberty, "DNA retention".
http://www.liberty-human-rights.org.uk/human-rights/privacy/dna-retention/index.php
[570] Section 64 (1A) of the PACE was substituted by Section 82 of the Criminal Justice and Police Act 2001.

creep, dangers of profiling, risk of endangering community relations. The collection and retention also gave "overriding and arguably unlimited control over the retention and subsequent use of the DNA sample/profile to the police force".[571]

Institutional response

The judiciary

The police took DNA samples and fingerprints from two individuals from Sheffield who subsequently challenged the retention of their DNA and fingerprint samples on the national DNA database (after one was acquitted and charges were dropped against the other), alleging a breach of Articles 8 and 14 of the European Convention on Human Rights. In both cases, the police had refused to destroy their data. The individuals applied for judicial review of the decision. The Administrative Court rejected their application,[572] and the Court of Appeal upheld its decision suggesting that the risks were "outweighed by the benefits in achieving the aim of prosecuting and preventing crime".[573] The House of Lords also dismissed an appeal by the individuals.[574] The matter was taken to the European Court of Human Rights (ECtHR) which found in its judgment of 4 December 2008 that

> the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.[575]

In 2011, the UK Supreme Court ruled that the ACPO guidelines (as amended) on the indefinite retention of DNA profiles were unlawful.[576] It stated that the legislature must be allowed a reasonable time in which to produce a lawful solution to a difficult problem and that if Parliament did not produce revised guidelines within a reasonable time, then the appellants would be able to seek judicial review of the continuing retention of their data under the unlawful ACPO guidelines and their claims would be likely to succeed.

Parliament

---

[571] Rodrigues, R. E., "Big Bio-Brother is here: wanting, taking and keeping your DNA", *Proceedings of the British and Irish Law, Education and Technology Association Conference,* Hertfordshire, April 2007. http://www.bileta.ac.uk/content/files/conference%20papers/2007/Big%20Bio-Brother%20is%20here%20-%20wanting,%20taking%20and%20keeping%20your%20DNA.pdf

[572] *R (S) v Chief Constable of South Yorkshire Police and the Secretary of State for the Home Department* and *R (Marper) v Chief Constable of South Yorkshire Police and the Secretary of State for the Home Department* [2002] EWHC 478 (Admin).

[573] [[2003] EWCA Civ 1275].

[574] *Regina v. Chief Constable of South Yorkshire Police ex parte LS* (by his mother and litigation friend JB) (FC) [2004] UKHL 39.

[575] *S and Marper v United Kingdom* [2008] ECHR 1581.

[576] R *(on the application of GC) (FC) v The Commissioner of Police of the Metropolis* [2011] UKSC 21 On appeal from: [2010] *ALL ER* D 174.

The post-ECtHR Marper situation was addressed through legislative changes. The main change was the introduction of the Protection of Freedoms Act 2012 (entry into force 1 May 2012) which regulates the use of biometric data. Sections 1-25 of the Act relate to DNA and fingerprint retention. The Act requires all DNA samples to be destroyed within six months of being taken. If a person has been arrested for a minor offence, but never convicted, any DNA and fingerprints taken by the police must be destroyed. The Act provides for the appointment of a Biometrics Commissioner[577] with the general responsibility of reviewing the retention and use of DNA and fingerprints, including applications for retention made on national security grounds.

Home Office

Post-ECtHR Marper, the Home Office launched a consultation in May 2009, the objective of which was "to develop a DNA framework which has the support and confidence of the public and achieves a proportionate balance between the rights of the individual and protection of the public".[578] Upon review, researchers at Lancaster University criticised the consultation document for containing "flawed statistical evidence".[579] The researchers' findings led the Home Office to review their evidence and policy and ultimately to issue a new policy report titled "DNA Retention Policy: Re-Arrest Hazard Rate Analysis".[580]

The Home Office carried out an equality impact assessment (EIA) on the "DNA & Fingerprints – New Framework for their Retention and Destruction" in 2011.[581] The EIA found that the proposed changes of the New Framework would "remove from the Database the majority of those who have not been convicted of an offence" and that "the proposed changes are unlikely to increase, either directly or indirectly, the proportion of such groups whose data is retained on the database; indeed, any impact should be positive in these areas by removing large number of such individuals".[582] It suggested that the "impact of these measures will be assessed as part of the ongoing process of assessing the equality impact of the NDNAD, carried out by the NPIA".[583] The process of the destruction of DNA samples (the biological material which contains all of a person's genetic information) began in December 2012. The Home

[577] The first Biometrics Commissioner, Alastair MacGregor QC, took up his post on 4 March 2013.
[578] Home Office, "Keeping the Right People on the DNA Database, Science and Public Protection", May 2009. A copy of the consultation is at: http://www.statewatch.org/news/2009/may/uk-ho-dna-consult.pdf
[579] Economic and Social Research Council, "Reviewing the DNA Database., http://www.esrc.ac.uk/impacts-and-findings/features-casestudies/case-studies/7724/reviewing-the-dna-database.aspx. The detailed pathway to impact is outlined in the full case study available at: http://www.esrc.ac.uk/_images/Reviewing%20the%20DNA%20database_tcm8-7727.pdf
[580] Home Office, "DNA Retention Policy: Re-Arrest Hazard Rate Analysis", 2009. http://webarchive.nationalarchives.gov.uk/20100418065544/http:/www.homeoffice.gov.uk/documents/cons-2009-dna-database/dna-retention-evidence-paper2835.pdf?view=Binary
[581] Home Office Crime and Policing Group, "DNA & Fingerprints – New Framework for their Retention and Destruction", 19 January 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/98397/dna-fingerprint-eia.pdf
[582] Ibid.
[583] Home Office Crime and Policing Group, "DNA & Fingerprints – New Framework for their Retention and Destruction", 19 January 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/98397/dna-fingerprint-eia.pdf

Office reports that DNA samples are being destroyed for all individuals (as at 4 April 2013, 439,000 DNA samples had been destroyed[584]), even those convicted of crimes, because of the sensitivity of the material and the fact that it is no longer needed once a DNA profile has been obtained. The Home Office reported that by the end of September 2013, all DNA and fingerprints not meeting the criteria of the Act would be destroyed. The deletion process operates on a continuous cycle so that new material, or material which has newly reached an expiry date, will be destroyed as well. At the end of this process (i.e., once all records held by the police and the databases are in accordance with the new laws), the Act's DNA and fingerprint provisions will officially come into force.[585]

Thus, we see the various institutional responses to the unlimited collection of samples and retention of profiles on the NDNAD and the ECtHR Marper decision. The judiciary in England and Wales (pre-ECtHR Marper) took a highly supportive stance towards the collection and retention of DNA focussing on the benefits of DNA in crime prevention and prosecution. Post-Marper, the judicial response was different (holding the ACPO guidelines unlawful). The more far-reaching response related to the legislative changes brought about in Parliament to address the situation and the actual practical effects in terms of actions taken by the Home Office: carrying out the EIA and the destruction of DNA samples. We see some movement from the approach of indiscriminately collecting and retaining DNA samples.

Societal response

Civil society organisations such as Liberty, GeneWatch and the Open Rights Group (ORG) were severely critical of the DNA collection and retention regime and resorted to a variety of actions. Liberty launched a DNA clinic to advise and help innocent young people in Hackney remove their DNA from the database.[586] GeneWatch monitored the situation, issued a position statement calling for "important changes that can be made to safeguard privacy and rights without compromising the use of DNA in fighting crime", issued press releases, reports,[587]briefings,[588] published articles,[589] and responded to official consultations.[590] The Open Rights Group (ORG)

[584] Home Office, "Protection of Freedoms Act 2012: how DNA and fingerprint evidence is protected in law", 4 April 2013. https://www.gov.uk/government/publications/protection-of-freedoms-act-2012-dna-and-fingerprint-provisions/protection-of-freedoms-act-2012-how-dna-and-fingerprint-evidence-is-protected-in-law

[585] Ibid.

[586] Liberty, "DNA retention".
http://www.liberty-human-rights.org.uk/human-rights/privacy/dna-retention/index.php

[587] GeneWatch, "The Police National DNA Database: Balancing Crime Detection, Human Rights and Privacy", 1 January 2005.

[588] GeneWatch, "The Police National DNA Database: Human rights and privacy", Briefing 31, 1 June 2005; GeneWatch, "Would 114 murderers have walked away if innocent people's records were removed from the National DNA Database?", June 2006; GeneWatch, "How many innocent children are being added to the National DNA Database?" *Police and Criminal Evidence Act (PACE) consultations briefing*, 22 May 2007; GeneWatch, "The DNA database: what next?" 2 July 2010, GeneWatch, "DNA Database: what can I do?"; GeneWatch, "The DNA database: contacting your MP", 31 October 2010; GeneWatch, "DNA databases and human rights", 12 January 2011; GeneWatch, "DNA database: analysis of offending figures", 7 November 2011. See http://www.genewatch.org/pub-492775.

[589] Wallace, Helen, "The UK National DNA Database: Balancing crime detection, human rights and privacy", *EMBO Rep*. 2006 July; 7(SI): S26–S30. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490298/. Wallace for instance, called for making

has a wiki on the DNA database to highlight problems and concerns in relation to the database.[591]

The media investigated and disseminated information and created greater public awareness on the collection and retention of DNA samples and fingerprints. They investigated, followed and disseminated information about new developments on this subject.[592] For example, BBC News dedicated a "Q & A" page to the National DNA Database;[593] it published various articles on the retention term of DNA samples,[594] criminalisation of people,[595] questioned the size and purpose of the database,[596] presented case studies on the role of DNA and the database,[597] and highlighted the need for a debate on the subject.[598] These are but some of the examples of the BBC news coverage as evident from their website (on searching for the NDNAD). Many people voiced their comments and expressed their opinions about these articles on these articles.

Bloggers (professional and amateur) posted information and stimulated debate on the unlimited collection and retention of samples and creation of profiles on the national DNA database.[599] This blogging activity represents a more versatile and dynamic form of stakeholder engagement (and even education). Twitter users posted entries on the ECtHR Marper decision,[600] the national DNA database (the posts include information about the database, calls for debate, concerns about the database, its Orwellian potential and support for it).

---

changes to "safeguard privacy and individuals' rights without compromising the use of DNA in tackling crime" through measures such as public debate, destruction of samples on completion of investigation, stoppage of controversial genetic research using the NDNAD, taking DNA samples only when an individual is charged, and creation of an independent, transparent and accountable governing body to monitor police use of DNA profiles and samples.

[590] See GeneWatch. http://www.genewatch.org/sub-539478

[591] Open Rights Group, "DNA Database". http://wiki.openrightsgroup.org/wiki/DNA_database

[592] For example, see *The Guardian*, "DNA Database". http://www.guardian.co.uk/politics/dna-database

[593] Casciani, Dominic, "Q&A: The national DNA database", BBC News, 7 May 2009. http://news.bbc.co.uk/2/hi/uk_news/7532856.stm

[594] BBC News, "Six-year limit on DNA of innocent", 11 Nov 2009. http://news.bbc.co.uk/2/hi/uk_news/politics/8354850.stm

[595] Joyce, Julian, "Innocent – but battling a DNA record", 28 February 2008. http://news.bbc.co.uk/2/hi/uk_news/7267421.stm; BBC News, "DNA records 'criminalise people'", 30 July 2008. http://news.bbc.co.uk/2/hi/uk_news/7531588.stm

[596] Silverman, Jon, "Has our DNA database gone too far?", 5 September 2007. http://news.bbc.co.uk/2/hi/uk_news/6979165.stm

[597] Casciani, Dominic, "DNA Database: Key case studies", BBC News, 7 May 2009. http://news.bbc.co.uk/2/hi/uk_news/8037972.stm

[598] Kelly, June, "DNA database debate urged", BBC News, 28 February 2008. http://news.bbc.co.uk/2/hi/uk_news/7259494.stm

[599] DNABoss. http://thednaboss.wordpress.com/blog/. A blog run by life science specialists; Katz, Deanne, "National DNA Database Comes under Scrutiny", *FindLaw,* February 2013. http://blogs.findlaw.com/blotter/2013/02/national-dna-database-comes-under-scrutiny.html; Wagner, Adam, "DNA Database: another key human rights election issue", *UK Human Rights Blog,* 19 April 2010. http://ukhumanrightsblog.com/2010/04/19/dna-database-another-key-human-rights-election-issue/. Palmer, Jessica, "EU court to Britain: your national DNA database violates human rights", *Bioephemera,* 11 Dec 2008. http://scienceblogs.com/bioephemera/2008/12/11/eu-court-to-britain-your-natio/

[600] A list of such tweets is available at: https://twitter.com/search?q=s%20and%20marper&src=typd

After the Marper decision in 2008, *The Guardian* highlighted how the Association of Chief Police Officers (ACPO) through a letter had advised senior police officers to "ignore a landmark ruling by the European court of human rights and carry on adding the DNA profiles of tens of thousands of innocent people" to the NDNAD.[601]

Academics of different backgrounds (science,[602] criminology, law,[603] philosophy,[604] political science) debated and discussed the regime from various perspectives. Williams, Johnson and Martin in their report on *Genetic Information and Crime Investigation* [605] highlighted that until 2004 "no comprehensive review of the robustness of the scientific and technical practices central to the operation of the NDNAD itself has ever been published in the scientific peer reviewed literature" and recommended "an authoritative review of the scientific and technological foundations of the NDNAD", alongside calling for "future policy discussions on the expansion and developing uses of the NDNAD", according priority and resources to independent evaluation of the effectiveness of police uses of the NDNAD, and creation of an independent oversight body with lay members to scrutinise the workings of the NDNAD.[606] McCartney explored the possible implications of the rapid expansion of the England and Wales National DNA Database (NDNAD) and highlighted how new risks are created, including not only error, improper access and disclosure and function creep but also the potential creation of a "suspect society" with forensic DNA technology co-opted into mass surveillance and social control mechanisms.[607] Lipscombe examined the NDNAD in the context of sexed violence (a concept that includes sexual crime and gendered and violent aspects of crimes) and called for improvements to the database while cautioning that "technologies of fear will only hinder criminal justice, not improve it."[608]

The S and Marper case (particularly post the 2008 ECtHR decision) stimulated further academic discussion on the collection and retention of DNA samples – for instance, as done by Hepple,[609] Beattie,[610] Pease,[611] McCartney[612] and Campbell.[613] Other (2011

---

[601] Travis, Alan, "Police told to ignore human rights ruling over DNA database", *The Guardian,* 7 Aug 2009. http://www.guardian.co.uk/politics/2009/aug/07/dna-database-police-advice

[602] E.g. Linacre, A.M.T., "The UK national DNA database", *Lancet,* 361 (9372), 2003, pp. 1841-1842.

[603] Rodrigues, R.E, "Big Bio-Brother is here: wanting, taking and keeping your DNA", *Proceedings of the British and Irish Law, Education and Technology Association Conference,* Hertfordshire, April 2007. http://www.bileta.ac.uk/content/files/conference%20papers/2007/Big%20Bio-Brother%20is%20here%20-%20wanting,%20taking%20and%20keeping%20your%20DNA.pdf

[604] Levitt, Mairi, "Forensic databases: benefits and ethical and social costs", *British Medical Bulletin* Vol.83, No. 1, 2007, pp. 235-248.

[605] Williams, Robin, P. Johnson and P. Martin, *Genetic Information and Crime Investigation: Social, ethical and public policy aspects of the establishment, expansion and police use of the National DNA Database,* Report, 2004.
http://www.dur.ac.uk/robin.williams/Williams_Johnson_Martin_NDNAD_report_2004.pdf

[606] For full set of recommendations, see the report. Williams, ibid.
http://www.dur.ac.uk/robin.williams/Williams_Johnson_Martin_NDNAD_report_2004.pdf

[607] McCartney, Carole I., "Forensic DNA Sampling and the England and Wales National DNA Database: A Sceptical Approach", *Critical Criminology,* Vol. 12, No. 2, 2004, pp. 157-178.

[608] Lipscombe, Sarah, "Challenging privacy: Using the National DNA Database to support victims of sexed violence", *Internet Journal of Criminology,* 2010.
http://www.internetjournalofcriminology.com/Lipscombe_Dissertation_April_2010.pdf

[609] Hepple, B., "Forensic databases: implications of the cases of S and Marper", *Medicine, Science and the Law*, Vol. 49, Issue 2, April 2009, pp. 77-87. This article talks about the Marper judgment and discusses issues such as the reliability of fingerprint and DNA evidence and its effectiveness in preventing and detecting crime.

onwards) academic publications have focused on young offenders and the future of the NDNAD,[614] compliance with human rights legislation,[615] potential contribution of criminal career research on DNA retention policies,[616] etc.

Conclusion

In this case, there was a threat (i.e., the unlimited collection and retention of DNA samples) to a democratic society and its principles and values such as privacy, data protection, right to equal treatment, individual liberty in addition to ethical concerns. The community, institutions and individuals reacted to the threat in different manners.

When exposed to this threat, society generally resisted – this is evident in the societal response. It also simultaneously absorbed and accommodated the effects of the threat due to perceived benefits– this is evident in the public support and institutional reactions to the threat and efforts to mitigate its effect. The absorptive and accommodative elements are also evident in the moves of institutional bodies to find a way to circumvent or restore the surveillance status quo.

The positive elements evident in this case are:

- Ability of society to organise quickly (galvanise to action)
- Ability to disseminate information and raise awareness (on an ongoing basis)
- Addressing threats across domains (including cross-domain collaborations)
- Positive social context (establishment and wide acceptance of privacy and data protection rights)
- Ability of civil society to lead, influence society and decision-makers
- Capacity of individuals to take action
- Availability of suitable redress forums.

Despite this, concerns remain and it is not clear whether the threat from the DNA surveillance under this regime has been effectively addressed. McCartney comments that while post-Marper "successive UK governments have drafted new retention

---

[610] Beattie, Kate, "S and Marper v. UK: Privacy, DNA and Crime Prevention", *European Human Rights Law Review*, Vol. 2, 2009, pp. 229-238.
[611] Pease, Ken, "DNA Retention after S and Marper", *Keeping the Right People on the DNA Database,* Consultation paper, Jill Dando Institute, 2009.
[612] McCartney, Carole I., "Of Weighty Reasons and Indiscriminate Blankets: The Retention of DNA for Forensic Purposes", *The Howard Journal of Criminal Justice*, Vol. 51, Issue 3, July 2012, pp. 245-260.
[613] Campbell, Liz, "DNA Databases and Innocent Persons: Lessons from Scotland?", *Juridical Review,* Vol. 4, 2010.
[614] Anderson, Claudine, Rebecca Stackhouse, Anita Shaw and Rachel Iredale, "The National DNA Database on trial: engaging young people in South Wales with genetics", *Public Understanding of Science*, Vol. 20, No. 2, March 2011, pp. 146-162.
[615] Blakemore, Brian, and Christopher Blake, "Can the National DNA Database be Effective and Comply with Human Rights Legislation?" *The Police Journal,* September 2012, Vol. 85, No. 3, pp. 191-202.
[616] Kazemian, L., K. Pease and D. P. Farrington, "DNA Retention Policies: The Potential Contribution of Criminal Career Research", *European Journal of Criminology*, Vol. 8, January 2011, pp. 48-64.

regimes but serious doubts remain as to whether the issue of DNA retention has been satisfactorily resolved".[617]

3.3.4 NSA revelations

David Wright, Trilateral Research & Consulting
Dr Reinhard Kreissl, Institute for the Sociology of Law and Criminology (IRKS)

Nature of the adverse event

Beginning in early June 2013, *The Guardian*, *The New York Times* and other media have reported in unprecedented detail on the surveillance activities of the US National Security Agency (NSA) and other intelligence services, based on documents leaked by Edward Snowden, an employee of defence contractor Booz Allen Hamilton at the NSA. The leaked documents revealed how extensively the intelligence agencies have been surveilling whole populations as well as political leaders, UN officials and businesses, such as Google, Petrobas and many others.

The leaks can be described as an adverse event for the intelligence agencies because the public now knows that the NSA has seriously infringed their privacy, ostensibly to hunt for terrorists, and that this mass and targeted surveillance has served to give national industries an economic advantage over their competitors. The surveillance has served other purposes too. The intelligence agencies have kept an eye on dissidents and civil society organisations who might disrupt social order. The leaks have been an adverse event for political leaders such as US President Barack Obama and UK Prime Minister David Cameron because the leaks have embarrassed them and strained their relations with supposed allies, such as German Chancellor Angela Merkel, European parliamentarians, Brazilian President Dilma Rousseff, Mexican President Enrique Peña Nieto and others. The leaks have been an adverse event for Verizon, AT&T, Google, Facebook and other businesses who have given access to their networks to the NSA, the public realisation of which has undermined public confidence in these companies and the adequacy of the security of their personal data held by these companies. The leaks have also been an adverse event for the public who have been shocked and outraged that the intelligence agencies have so extensively invaded their privacy.

This section explores the European institutional, judicial, legal, societal, economic and media responses to the so-called Snowden revelations. While the emphasis of this section is on the European impacts, the paper references some non-European responses where they seem to be particularly noteworthy. It references only a selection of the many reports based on the leaked documents and only up to the end of November 2013, so it is, of course, by no means comprehensive, but enough evidence is presented here to allow us to draw some conclusions about the impacts of the Snowden revelations. While the revelations have been a shock to many, if not most people, they have had some unintended, positive impacts, which we identify. The section concludes with some observations about the failure of oversight, the privacy-security trade-off paradigm and the breakdown of open democracy. It also poses some

[617] McCartney, Carole I., "Of Weighty Reasons and Indiscriminate Blankets: The Retention of DNA for Forensic Purposes", *The Howard Journal of Criminal Justice*, Vol. 51, Issue 3, July 2012, pp. 245-260.

unanswered questions and makes some recommendations on protecting privacy in a surveillance society.

On 5 June 2013, *The Guardian* published its first exclusive, revealing that the US Foreign Intelligence Surveillance Court ("the FISA court") had granted a secret order forcing Verizon, one of the largest of US telecom companies, to give the NSA access to the phone records of millions of Americans. The NSA would thus have information on all landline and mobile telephone calls in the Verizon network, both within the US and between the US and other countries. *The Guardian* said the Obama administration was collecting the communication records of millions of US citizens, regardless of whether the people were suspected of any wrongdoing.[618] Following the 11 September 2011 attacks, the Bush administration had greatly expanded surveillance of the US population, and the Obama administration has expanded that surveillance even more.

The NSA was collecting "metadata" not only from telecom companies, but also from Internet social networks. On 6 June 2013, *The Washington Post* reported the existence of a secret programme code-named PRISM, under which the NSA was collecting e-mails, Internet phone calls, photos, videos, file transfers and social-networking data from Google, Facebook, Apple, YouTube, Skype, Microsoft and PalTalk.[619] According to NSA watcher James Bamford, the agency runs its intercepts of millions of telephone calls and e-mails through powerful computers that screen them for particular names, telephone numbers, Internet addresses, and trigger words or phrases. Any communications containing flagged information are forwarded by the computer for further analysis.[620]

On 9 June, Edward Snowden revealed that he had leaked the documents.[621] He justified his actions by saying that he did "not want to live in a world where everything I do and say is recorded". He said that the public, not spies and secret courts, ought to decide whether the mass surveillance was right. According to *The Guardian*, "he chose to reveal himself to avoid hiding behind the secrecy he abhors".[622]

On 21 June 2013, *The Guardian* reported that the UK's Government Communications Headquarters (GCHQ) had secretly gained access to the cable networks that carry the world's phone calls and Internet traffic and had been "processing vast streams of sensitive personal information which it was sharing with the NSA without any form

---

[618] Associated Press, "Obama administration collecting huge number of citizens' phone records, lawmaker says", 6 June 2013. http://www.washingtonpost.com/politics/federal_government/report-government-secretly-scooping-up-phone-records-of-millions-of-verizon-customers/2013/06/05/e820deb8-ce57-11e2-8573-3baeea6a2647_story.html

[619] *The Economist*, "Surveillance: Look who's listening", 15 June 2013. http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[620] Bamford, James, "Big Brother Is Listening", *The Atlantic*, 1 Apr 2006. http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/?single_page=true

[621] The Economist, op. cit., 2013.

[622] The Economist, op. cit., 2013.

of public acknowledgement or debate". The GCHQ programme was codenamed TEMPORA.[623]

On 9 August 2013, President Obama said that "The people at the NSA don't have an interest in doing anything other than making sure that ... we can prevent a terrorist attack." Yet leaked documents soon showed that the NSA had also been spying on its "allies", including European Union offices, the United Nations (including UN Secretary General Ban ki-moon) and the International Atomic Energy Agency. The NSA has infiltrated the EU mission to the UN in New York and the EU embassy in Washington. The documents revealed that the NSA had secret eavesdropping posts in 80 US embassies and consulates around the world, internally referred to as the "Special Collection Service" (SCS) and jointly operated with the CIA.[624] On 30 October, *The Washington Post* reported that the NSA had secretly broken into the unencrypted fibre-optic cables that carry data between Google and Yahoo's data centres around the world, without the companies' knowledge.[625] In other words, the NSA has had both legal and illegal access to Google's networks. The NSA's principal tool to exploit the data links is a project called MUSCULAR, operated jointly with the GCHQ. Google and Yahoo presumably have concerns that reports that the NSA has intercepted data between their servers will erode people's trust in the companies' ability to keep their data confidential.

While the Snowden revelations created a huge media storm, they were not entirely novel. More than a decade before, news of the secret Echelon programme came to light and was the subject of an inquiry by the European Parliament.[626] The FBI had been operating a programme called Carnivore authorised by the 1994 Communications Assistance for Law Enforcement Act (CALEA) which obliged telecom operators to provide it access to their communications networks. However, what made the Snowden revelations different was the scale of the NSA's spying on ordinary citizens who had never committed any crime, nor even been suspected of having committed any crime. The furore was compounded further because the surveillance had been conducted under secret authorisation. Undoubtedly, the scale of surveillance is a function of new technologies. Had the Internet existed at the time of Echelon, the intelligence agencies may well have indulged in much greater spying in those days too. Thus, it could be argued that what has changed is capability of the techno-infrastructure of communication rather than a presumed increase in the intelligence services' desire to spy on citizens. More likely, the NSA et al. take

[623] MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian*, 21 June 2013. http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[624] Poitras, Laura, Marcel Rosenbach and Holger Stark, "Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[625] Gellman, Barton, and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", *The Washington Post*, 30 October 2013. http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?hpid=z1

[626] European Parliament, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), 11 July 2001. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=EN

whatever they can get and if the technology provides new opportunities, they take them.

Thus, the Verizon story was just the tip of a gigantic surveillance iceberg. While some people were aware that the NSA and other intelligence agencies were monitoring telephone calls and Internet use[627], the sheer scale of the NSA surveillance was breath-taking. It seemed that the NSA, with some help from the GCHQ, was monitoring virtually everyone's telephone calls and Internet usage.

Institutional response

A few days after the Snowden revelations began, President Obama met President Xi Jinping of China in southern California. Obama was going to complain about Chinese cyberattacks and spying, which had attracted a fair amount of media attention in the months (and even years) before Obama's meeting, but the huge media coverage of US spying completely defocussed attention on Chinese spying. The fury over the extent of NSA surveillance has distracted US efforts at applying pressure on China to rein back its cyber espionage activities. Once the NSA revelations began, Chinese cyber surveillance disappeared from the front pages of newspapers.

On 8 June 2013, US Director of National Intelligence James Clapper issued a public statement acknowledging PRISM's existence, but stressing that it was lawful and operated under the auspices of the FISA court. Just three months earlier, in March 2013, Clapper had testified under oath before the US Senate where he said the NSA did not intentionally collect "any type of data at all" on millions of Americans. That turned out to be not true. Clapper later justified his response as the "least untruthful answer" he could give.[628] Amid revelations that the NSA does indeed collect large amounts of citizens' data and metadata, he subsequently apologised, saying his previous answer was "erroneous".[629]

The head of the NSA, Army Gen. Keith Alexander, also initially denied that the United States collected telephone and e-mail records directly from European citizens, calling reports based on leaks by Edward Snowden "completely false". Subsequent leaks showed that Alexander was also misleading the public and not being truthful.[630]

This section reviews a few of the key institutional responses to the NSA revelations, notably the fury they caused in Europe when it became apparent that the NSA was not only sweeping up the communications of ordinary citizens, but also targeting European and other leaders such as the Bolivian, Brazilian and Mexican presidents, supposedly close allies.

---

[627] James Bamford wrote extensively about NSA surveillance in his book *The Shadow Factory*, published by Anchor Books in July 2009, four years before the Snowden revelations.

[628] Rusbridger, Alan, "The Snowden Leaks and the Public", *The New York Review of Books*, 21 November 2013 issue. http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/?pagination=false

[629] *The Economist*, "Sense, sensibilities and spying", 6 July 2013.
http://www.economist.com/news/international/21580485-edward-snowdens-revelations-about-american-espionage-have-riled-europeans-so-has?zid=301&ah=e8eb01e57f7c9b43a3c864613973b57f

[630] Ball, James, "Separate draft memo proposes US spying on 'Five-Eyes' allies", *The Guardian*, 20 Nov 2013.
http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data

European fury

After news of the NSA's PRISM programme became public, European lawmakers threatened to abandon data sharing agreements with the United States. Members of the European Parliament (MEPs) were described as "furious" that US authorities had been accessing their e-mails and other personal data from leading Internet companies. In a heated debate in the European Parliament, lawmakers complained that for a decade they had bowed to US demands for access to European financial and travel data and said it was now time to re-examine the deals and to limit data access. "We need to step back here and say clearly: mass surveillance is not what we want," said Green Member of the European Parliament (MEP) Jan Philipp Albrecht.[631]

Other members of the European Parliament said they would redouble efforts to strengthen a proposed EU-US data protection agreement in the field of police and judicial co-operation.[632] European Commission Vice President Viviane Reding also said that "Programmes such as PRISM… potentially endanger the fundamental right to privacy and to data protection of EU citizens." EU officials demanded "swift and concrete answers" from the US government about its spying programs.[633] Following revelations of GCHQ's TEMPORA surveillance programme, Ms Reding also sent a letter to UK foreign minister William Hague asking for details. She asked if TEMPORA is restricted to national security, if snooping is limited to individual cases or is in bulk, if the data is shared with third countries like the United States, and if UK and EU citizens have any legal recourse when it comes to their data.[634] Five months later, she still had not received a response.

Member States: US Mass Surveillance is "Monstrous"

The fury at European level was mirrored at the level of EU Member States too. Peter Schaar, German Federal Commissioner for Data Protection, said, "The U.S. government must provide clarity regarding these monstrous allegations of total monitoring of various telecommunications and Internet services." He added that "Statements from the US government that the monitoring was not aimed at US citizens but only against persons outside the United States do not reassure me at all."[635]

---

[631] Davenport, Claire, "U.S. PRISM spying programme rattles EU lawmakers", Reuters, 11 June 2013. http://in.reuters.com/article/2013/06/11/usa-security-eu-idINL5N0EN1D4201306112

[632] Watt, Nicholas, "Prism scandal: European commission to seek privacy guarantees from US", *The Guardian*, 10 June 2013. http://www.guardian.co.uk/world/2013/jun/10/prism-european-commissions-privacy-guarantees

[633] Bracy, Jedidiah, "NSA Leaks: EU-U.S. Tensions on the Rise, Europe Reacts", *The Privacy Advisor*, International Association of Privacy Professionals (IAPP), 13 June 2013. https://www.privacyassociation.org/publications/nsa_leaks_eu_u.s._tensions_on_the_rise_europe_reacts_roundup

[634] Nielsen, Nikolaj, "EU asks for answers on UK snooping programme", EUObserver.com, 26 June 13. http://euobserver.com/justice/120656

[635] EurActiv, "US data scandal deepens EU-US divide on privacy", 10 June 2013. http://www.euractiv.com/infosociety/us-data-scandal-deepens-eu-us-di-news-528437?utm_source=EurActiv%20Newsletter&utm_campaign=47551f8aa6-newsletter_daily_update&utm_medium=email&utm_term=0_bab5f0ea4e-47551f8aa6-245739993

French prosecutors announced that they were conducting a preliminary investigation into whether the NSA had violated French law by secretly collecting personal data.[636] The espionage is "absolutely unacceptable", inveighed French Foreign Minister Laurent Fabius after it became known that the French embassy in Washington was also on the surveillance list.[637]

The UK's Information Commissioner's Office (ICO) said, "There are real issues about the extent to which U.S. law enforcement agencies can access personal data of UK and other European citizens. Aspects of U.S. law under which companies can be compelled to provide information to U.S. agencies potentially conflict with European data protection law, including the UK's own Data Protection Act." The ICO also said it "has raised this with its European counterparts, and the issue is being considered by the European Commission, who are in discussions with the U.S. government."[638]

But, as noted above, the NSA was not the only intelligence agency conducting surveillance outside its borders. German justice minister Sabine Leutheusser-Schnarrenberger commented that if reports about TEMPORA proved to be true, it would be "a Hollywood nightmare". She sent a letter to British home secretary Theresa May and justice secretary Chris Grayling asking if media reports were true.[639]

GCHQ had tried to reassure citizens that "GCHQ takes its obligations under the law very seriously." A spokesman added, "Our work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight, including from the Secretary of State, the Interception and Intelligence Services Commissioners and the Intelligence and Security Committee."[640]

UK Foreign Secretary William Hague also insisted that UK intelligence agencies practise and uphold UK law at all times. He said there are two acts of Parliaments governing the process of obtaining permission for the security services to eavesdrop, which require a signed warrant from the Foreign or Home Secretary, and must be "necessary, proportionate and carefully targeted". They are also subject to review by

---

[636] Associated Press, "French prosecutor opens probe into NSA surveillance program", published in *The Washington Post*, 28 Aug 2013. http://www.washingtonpost.com/world/europe/french-prosecutor-opens-probe-into-nsa-surveillance-program/2013/08/28/8f63d06e-0ff2-11e3-a2b3-5e107edf9897_story.html

[637] Poitras, Laura, "Marcel Rosenbach and Holger Stark, Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[638] Bracy, Jedidiah, "NSA Leaks: EU-U.S. Tensions on the Rise, Europe Reacts", *The Privacy Advisor*, IAPP. International Association of Privacy Professionals, 13 June 2013. https://www.privacyassociation.org/publications/nsa_leaks_eu_u.s._tensions_on_the_rise_europe_reacts_roundup

[639] Nielsen, Nikolaj, "EU asks for answers on UK snooping programme", EUObserver.com, 26 June 13. http://euobserver.com/justice/120656

[640] Hope, Christopher, and Tom Whitehead, "British Intelligence watchdog flies to Washington to demand answers on snooping scandal", *The Telegraph*, 7 June 2013. http://www.telegraph.co.uk/technology/internet-security/10107059/British-Intelligence-watchdog-flies-to-Washington-to-demand-answers-on-snooping-scandal.html

an independent commissioner to ensure permission is compliant with law.[641] Hague told MPs that British spies did not "indiscriminately trawl" through their citizens' e-mails or use foreign intelligence to bypass their own legal safeguards. "It has been suggested GCHQ uses our partnership with the United States to get around UK law, obtaining information that they cannot legally obtain in the UK," Mr Hague said. "I wish to be absolutely clear that this accusation is baseless."[642]

More recent disclosures belie the assurances from GCHQ and the government. An investigation by *The Guardian* and Channel 4 News discovered that GCHQ and the NSA reached an agreement in 2007 that allowed the NSA to access, analyse and store the phone, Internet and e-mail records of British citizens. Sir Malcolm Rifkind, chairman of the parliamentary Intelligence and Security Committee, told *The Guardian* that he would be seeking an explanation about the secret deal that appeared to allow the NSA to "unmask" personal data about Britons not suspected of any wrongdoing.[643]

Why were the leaders of the allied countries targeted?

Predictably, the heads of the intelligence agencies initially said their actions were aimed at protecting their countries against the threat of terrorism[644], but that hasn't explained why they were targeting the leaders of Germany, Italy, Spain and other allies. *Die Zeit*, the German weekly newspaper, carried a lead article on 31 October 2013, in which the writer Heinrich Wefing claimed, "The U.S. secret service has treated the chancellor as if she was an enemy herself" and that "This is exactly why 'cellphone-gate' marks a fundamental rupture" in German-US relations.

The NSA surveillance of political leaders of allied countries might have occurred simply because the NSA has the technology to do it. US Secretary of State John Kerry seems to have admitted as much when he acknowledged in a video conference on open government in London that "There is no question that the president and I and others in government have actually learned of some things that had been happening, in many ways, on an automatic pilot because the technology is there."[645] More likely,

---

[641] Settle, Michael, "Hague tells MPs claims of illegal spying are baseless", *The Herald* [Scotland], 11 June 2013.
http://www.heraldscotland.com/politics/political-news/hague-tells-mps-claims-of-illegal-spying-are-baseless.21306152

[642] Warrell, Helen, and James Blitz, "David Cameron rejects claims GCHQ broke law over US Prism data", *The Financial Times*, 10 June 2013.
http://www.ft.com/cms/s/0/01d745fe-d1f0-11e2-b17e-00144feab7de.html#axzz2VsHkbdAE

[643] Hopkins, Nick, and Matthew Taylor, "Watchdog demands GCHQ report on NSA's UK data storage", *The Guardian*, 21 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/21/sir-malcolm-rifkind-gchq-report-nsa-data-storage

[644] Roberts, Da, and Spencer Ackerman, "White House offers tentative support for plans to rein in NSA surveillance", *The Guardian*, 29 Oct 2013.
http://www.theguardian.com/world/2013/oct/29/white-house-supports-nsa-review

[645] Associated Press, "Kerry: Some NSA surveillance work reached 'too far' and will be stopped", *The Washington Post*, 1 November 2013.
http://www.washingtonpost.com/politics/federal_government/kerry-some-nsa-surveillance-work-reached-too-far-and-will-be-stopped/2013/11/01/37aeba76-42fd-11e3-b028-de922d7a3f47_story.html

however, the NSA surveilled allies in order to assess what the allies were thinking and planning to do in a range of different spheres, including the economic sphere.[646]

A breakdown of trust

When people became aware of how massive the surveillance of virtually everyone had become, among the reactions was not only outrage and fury, but also of an "enormous loss of trust", as Elmar Brok, the chairman of the Foreign Affairs Committee at the European Parliament, put it.[647] The theme of trust was repeated by many others. For example, German federal data protection commissioner Peter Schaar was quoted as saying that "If we want to return to a relationship based on trust, it will require serious effort… Officially the Americans said that they respected German law. Now we know that was not the case."[648]

The breakdown of trust is often accompanied by embarrassment, but the embarrassment was not just in Washington. The revelations also caused embarrassment in Europe. In the summer of 2013, German Chancellor Angela Merkel defended the US, when it became known that the NSA had the whole of the German population as a target of mass surveillance. But when Merkel discovered that the US had been listening in on even her mobile calls, she rose to anger. However, she also found herself, somewhat embarrassingly, having to fend off criticism within her country that she had failed to react vigorously to the initial disclosures of extensive American eavesdropping on millions of Germans, and really became engaged only after her own personal privacy was violated.[649]

Merkel demanded that Washington reach a "no-spying" agreement with Berlin and Paris by the end of 2013, even though more than 90 per cent of Germans think that the Americans would breach a no-spying agreement anyway and continue their surveillance activities, according to a survey by public broadcaster ARD and *Die Welt*.[650]

US federal regulators have recognised that the NSA revelations have been damaging to US-Europe relations: Federal Trade Commissioner Julie Brill said (in October

---

[646] Leaked documents showed that the NSA spied on G20 leaders in Canada and London. Freeze, Colin, "Ottawa allowed U.S. to spy on G20 summit in Toronto, Snowden leak reveals", *The Globe and Mail*, 27 Nov 2013, last updated 28 Nov 2013.
http://www.theglobeandmail.com/news/politics/snowden-leak-reveals-us-spied-during-g20-summit-in-toronto/article15645575/

[647] Poitras, Laura, "Marcel Rosenbach and Holger Stark, Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[648] Landler, Mark, and David E. Sanger, "Obama May Ban Spying on Heads of Allied States", *The New York Times*, 29 Oct 2013.
http://www.nytimes.com/2013/10/30/world/europe/obama-may-ban-spying-on-heads-of-allied-states.html?_r=0

[649] Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html

[650] RT, "Germans lose trust in US, see NSA whistleblower Snowden as hero – poll", *RT,* 8 Nov 2013.
http://rt.com/news/germany-lose-trust-us-snowden-431/

2013): "There is no doubt that the revelations about the National Security Agency's surveillance programs have severely tested the close friendship between the United States and many of our European colleagues."[651]

The intelligence committees of both the US Senate and House of Representatives have initiated hearings on the NSA practices. Bipartisan legislation calling for reform of the NSA has been introduced in both the House and Senate. President Barack Obama said his administration was conducting a complete review of intelligence activities.[652]

The European Parliament's LIBE committee on Civil Liberties, Justice and Home Affairs has been conducting its own investigation into the surveillance operations. As part of its investigation, it travelled to Washington, DC, to meet with officials from the State Department, Capitol Hill, various intelligence agencies and White House staff to discuss the impact that US surveillance programs have had on EU citizens. As of the end of November 2013, it is not clear what results these various hearings will achieve.

Involvement of other agencies in the mass surveillance

European politicians have sought to play down the role their own security services have played in secret surveillance. The UK's response or, at least, that of David Cameron, to the NSA revelations has been somewhat muted, probably because GCHQ has long co-operated with the NSA, often carrying out surveillance on behalf of the United States.[653] The Snowden revelations crossed the border between front stage and back stage politics. We can assume that most surveillance agency staff and their immediate stakeholders were aware of what was going on, but this was not a legitimate topic of public policy discourse. Bringing this "tacit" background knowledge to the foreground created a severe disturbance of policy. It is like the Mafia "Omerta" code: as long as all involved keep their secrets to themselves, the system works.

Although there has been considerable righteous indignation in Europe about the NSA surveillance, the security services in Germany, France, Spain and Sweden, and perhaps elsewhere have also been carrying out mass online surveillance and wiretapping[654] – not as extensively as the NSA and GCHQ, but mass surveillance

---

[651] Romm, Tony, and Erin Mershon, "EU to D.C.: Friends 'do not spy on each other'", Politico, 29 Oct 2013. http://www.politico.com/story/2013/10/european-union-nsa-friends-do-not-spy-on-each-other-99035.html

[652] Roberts, Da, and Spencer Ackerman, "White House offers tentative support for plans to rein in NSA surveillance", *The Guardian*, 29 Oct 2013. http://www.theguardian.com/world/2013/oct/29/white-house-supports-nsa-review

[653] Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html. For a readable history of the collaboration between GCHQ and the NSA (and its antecedents), see Aldrich, Richard, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency,* Harper Press, 2011.

[654] Borger, Julian, "GCHQ and European spy agencies worked together on mass surveillance", *The Guardian*, 1 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden. See also *Deutsche Welle*, "Germany admits Europe's spy agencies

nevertheless. According to a report in *The Guardian*, the German spy agency BND[655] had "huge technological potential and good access to the heart of the Internet".

US intelligence officials have insisted the mass monitoring in Europe was carried out by the security agencies in the countries involved and shared with the US.[656] However, US Director of National Intelligence James Clapper has acknowledged that the scale of surveillance by the NSA, with its 35,000 employees and $10.8 billion a year budget, sets it apart: "There's no question that from a capability standpoint we probably dwarf everybody on the planet, just about, with perhaps the exception of Russia and China."[657]

Judicial and legal consequences

This section discusses several judicial and legal consequences of the NSA revelations, i.e., the legal secrecy underpinning US surveillance, the attempts to remove an anti-FISA provision from the proposed EU Data Protection Regulation, the botched Safe Harbor Agreement, the circumventing of laws, Brazil and Germany's resolution to the UN, a study that finds mass surveillance violates EU law and, finally, the UK government's characterisation of David Miranda as a terrorist.

Legal secrecy

The US and UK governments have provided legal cover for some of the NSA and GCHQ's surveillance activities. Institutions like FISA provide a prima facie legal basis for many NSA actions, but they hollow out the idea of rule of law by doing so. Both in the US and in the UK, the legal secrecy that surrounds surveillance by the NSA and GCHQ is such that no company dares come out openly and discuss its relations with the secret services. In fact, it is illegal to do so.[658] In the US, the companies are legally required to share the data under the Foreign Intelligence Surveillance Act.[659] Nine US companies – Google, Microsoft, Yahoo, Facebook, PalTalk, YouTube, Skype, AOL, Apple – gave the NSA access to their client data[660], but company spokespersons said they had no knowledge of a government program providing officials with access to their servers, and drew a line between giving the

---

cooperate on surveillance", 2 Nov 2013. http://www.dw.de/germany-admits-europes-spy-agencies-cooperate-on-surveillance/a-17200903

[655] BND stands for Bundesnachrichtendienst or, in English, the Federal Intelligence Agency.

[656] Borger, Julian, "GCHQ and European spy agencies worked together on mass surveillance", *The Guardian*, 1 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.

[657] Shane, Scott, "No Morsel Too Minuscule for All-Consuming N.S.A.", *The New York Times*, 2 Nov 2013.
http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?src=un&feedurl=http%3A%2F%2Fjson8.nytimes.com%2Fpages%2Fworld%2Feurope%2Findex.jsonp

[658] Rusbridger, op. cit.

[659] Cain Miller, Claire, "Tech Companies Concede to Surveillance Program", *The New York Times*, 7 June 2013.
http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html

[660] Greenwald, Glenn, and Ewen MacAskill, "NSA taps in to systems of Google, Facebook, Apple and others, secret files reveal", *The Guardian*, 7 June 2013.
http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data?CMP=EMCNEWEML6619I2

government wholesale access to their servers to collect user data and giving them specific data in response to individual court orders. Google, Microsoft and Twitter publish transparency reports detailing government requests for information, but these reports do not include FISA requests because they are not allowed to acknowledge them.[661] Arguably, there is an irony of legal reasoning here: the law determines that you have to provide access to your data and at the same time it contains a clause stating that you are not allowed to tell anyone that you do: so the law has a built-in rule that says you are not allowed to tell anyone that you are acting according to legal rules.

The 1978 Foreign Intelligence Surveillance Act (FISA) established the FISA court, comprising 11 judges appointed by the chief justice of the United States, as a secret part of the federal judiciary. The FISA court approves or denies government requests to listen to foreigners' calls on the ground of national security. Snowden leaked documents showing that the FISA court had instructed Verizon to hand over information about all calls on its network "on an ongoing daily basis".

Section 215 of the PATRIOT Act allows the FBI or others to apply to the FISA court for a secret order compelling companies to turn over "any tangible things", as long as they are "relevant to an authorised preliminary or full investigation to obtain foreign intelligence information not concerning a US person". Section 215 allows the FBI to obtain information from a company about their customers, ostensibly "to protect against international terrorism or clandestine intelligence activities". The company must hand over that information to the investigators under a gag order that prevents them from ever informing the customer that the company even received the order.

The Economist sarcastically commented that authorities seem to believe that obtaining records of every telephone call made in America is either relevant to an investigation or an essential bulwark against international terrorism.[662]

As for PRISM, on paper, the protections against privacy abuse seem robust. Supposedly, the government does not unilaterally obtain information from company servers, nor does it target anyone for information-gathering without "an appropriate, and documented foreign-intelligence purpose to the acquisition". Also supposedly, it does not intentionally target any American citizen. The process is monitored by a FISA court, by Congress (through twice-yearly reports) and by independent inspectors-general. The information is subject to "minimisation procedures", designed to protect Americans unconnected to an investigation whose information is accidentally gathered.[663] However, the Snowden revelations have shown these suppositions to be wholly without merit.

---

[661] Cain Miller, Claire, "Tech Companies Concede to Surveillance Program", *The New York Times*, 7 June 2013.
http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html

[662] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[663] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

FISA orders do not give the government the right to listen to the content of calls. For that, law-enforcement agents need a separate warrant which requires suspicion of particular individuals and proof that "normal investigative procedures have been tried and failed". Instead, the NSA has collected metadata, the records of who people call, when, for how long, and so on.[664] However, computerised analysis of metadata can now provide a detailed portrait of who people know, where they go and their daily routines,[665] which is almost good or perhaps even better than intercepting the content of communications.[666]

When it became known that the NSA sweeps us some 5 billion records every day about the location data for hundreds of millions of mobile phones worldwide, an NSA spokesperson said the collection of the global mobile phone location data is legally authorised under Executive Order 12333, which governs all US espionage. That means congressional committees and relevant inspectors general can oversee the programme, but the secret court established under the Foreign Intelligence Surveillance Act (FISA) would not.[667]

The toothless FISA court

The reality is that the FISA seems to give virtually free reign to the NSA and FBI. Between 18 May 1979 and the end of 2004, the FISA court granted 18,742 NSA and FBI applications; it turned down only four outright.[668] In 2012, the government made 1,856 applications for electronic surveillance to FISA, and none was denied.[669] Thus, the government met formal legal requirements but the legal requirements were essentially a smokescreen to allow the NSA to do as it wished.

Despite the apparent weakness of the FISA court, President Bush secretly decided in 2001 that the NSA would no longer be bound by the FISA. Until then, before the NSA could place the name of an American on its watch list, it had to go before a FISA-court judge and show that it had probable cause to believe an individual was somehow connected to terrorism in order to get a warrant. Under Bush's new procedures, warrants do not always have to be obtained, and the critical decision

---

[664] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[665] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[666] For a good, brief description of how much metadata can reveal about a person, see Lithwick, Dahlia, and Steve Vladeck, "Taking the "Meh" out of Metadata", *Slate*, 22 Nov 2013.
http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html

[667] Associated Press, "NSA defends global mobile phone tracking as legal", published in *Gulf News*, 7 Dec 2013.
http://gulfnews.com/news/world/usa/nsa-defends-global-mobile-phone-tracking-as-legal-1.1264432

[668] Bamford, James, "Big Brother Is Listening", *The Atlantic*, 1 Apr 2006.
http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/?single_page=true

[669] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

about whether to put an American on a watch list is left to the vague and subjective "reasonable belief" of an NSA supervisor.[670]

The FISA Amendments Act of 2008 allows the US government to obtain an order from a national security court to conduct surveillance of foreigners abroad without individualised warrants even if the interception takes place on American soil.[671] Congress authorised the PRISM program and maintained that it minimises the collection and retention of information "incidentally acquired" about Americans and permanent residents. Several of the Internet companies said they did not allow the government open-ended access to their servers but complied only with specific lawful requests for information.

The law, which Congress re-authorised in late 2012, is controversial in part because Americans' e-mails and phone calls can be swept into a database without an individualised court order when they communicate with people overseas. While newspapers claimed the leaked documents showed that the NSA obtained direct access to the companies' servers, several of the companies, including Google, Facebook, Microsoft and Apple, denied that the government could do so. Instead, the companies said they had negotiated with the government technical means to provide specific data in response to court orders.[672] However, in October 2013, more leaked documents showed that the NSA was directly tapping into the companies' servers without the companies' knowledge.

The US government can rely on still other legislation to conduct secret surveillance. As mentioned above, the 1994 Communications Assistance for Law Enforcement Act (CALEA) required telephone companies to provide the government with secret access to their networks. The FCC has now extended the act to cover "any type of broadband Internet access service" and the new Internet phone services and ordered company officials never to discuss any aspect of the program.[673]

Watering down the proposed Data Protection Regulation

On 29 November 2011, someone leaked a draft of the proposed EU Data Protection Regulation, which contained a provision (Article 42.1) as follows:

> No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.

---

[670] Bamford, James, "Big Brother Is Listening", *The Atlantic*, 1 Apr 2006. http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/?single_page=true

[671] Savage, Charlie, Edward Wyatt and Peter Baker, "U.S. Says It Gathers Online Data Abroad", *The New York Times*, 6 June 2013. http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?hp&_r=1&

[672] Savage, Charlie, Edward Wyatt and Peter Baker, "U.S. Says It Gathers Online Data Abroad", *The New York Times*, 6 June 2013. http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?hp&_r=1&

[673] Bamford, James, "Big Brother Is Listening", *The Atlantic*, 1 Apr 2006. http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/?single_page=true

In point of fact, this provision meant that Europe would not recognise an order from the FISA court requiring a company to turn over European data to the US government, at least not without some kind of formal agreement with the EU. Article 42.1 would have eviscerated the FISA's power, at least as far as Europeans are concerned, by nullifying "any US request for technology and telecoms companies to hand over data on EU citizens".[674]

But between 29 November 2011 when a draft of the proposed Regulation was leaked and 25 January 2012, when the proposed Regulation was officially released, the US was successful in lobbying against the so-called "anti-FISA" clause and getting it removed.

The NSA revelations have occurred at a time when the European Parliament continues its consideration of the proposed Regulation. Until the Snowden revelations, US lobbyists, including those representing Google, Facebook, Microsoft, Amazon and Yahoo, had been successful in watering down various provisions of the proposed Regulation and in getting Europe to abandon Article 42.1, a measure that would have shielded Europeans from requests by American authorities to share online data gathered by some of the biggest American Internet companies. However, the Snowden revelations made parliamentarians realise that the proposed Regulation needed, if anything, to be stronger. European Commission Vice President Viviane Reding, among others, seized on the NSA revelations as justification for more stringent European data protection rules.

Hence, when the proposed Regulation emerged from the European Parliament's LIBE committee in October 2013, the above clause had been restored, word for word. It would forbid US companies from complying with US government requests for Europeans' personal data unless expressly approved by EU authorities. Since American companies can't agree to rules that would require them to ignore lawful US requests for information, the provision could effectively undermine US-EU data transfers.[675]

Restoration of the provision was a serious reversal for Washington. Furthermore, American technology companies worry that fines for breaking those rules and others could run as high as 5 per cent of a company's global annual revenue or €100 million, whichever is higher,[676] a provision that emerged from the LIBE committee in October 2013, which is somewhat stronger than the 2% figure mentioned in the January 2012 draft of the Regulation.

Safe Harbor agreement in danger of sinking

---

[674] Meyer, David, "U.S. secretly watered down Europe's proposed privacy rules, report claims", GigaOm, 13 June 2013. http://gigaom.com/2013/06/13/u-s-secretly-watered-down-europes-proposed-privacy-rules-report-claims/

[675] Mershon, Erin, "U.S. to EU: Don't scapegoat Safe Harbor over NSA", *Politico*, 7 Nov 2013. http://www.politico.com/story/2013/11/us-european-union-safe-harbor-nsa-99495.html?hp=l11

[676] Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html

The Snowden revelations have put the proposed Safe Harbor agreement in trouble – again. The Safe Harbor agreement between the US and EU came into operation in 2000 after the EU determined that US standards were "inadequate" in meeting the data protection principles of the EU's Data Protection Directive of 1995. The agreement allows US companies that want to handle or store European citizens' data to self-certify annually with the Department of Commerce that they will abide by the standards. The FTC is tasked with enforcing breaches of that agreement. European regulators became more vocal in their criticism of the framework following the first Snowden revelations, pointing out that Safe Harbor specifically provides for exemptions "to the extent necessary to meet national security, public interest or law-enforcement requirements". However, such exemptions are a kind of Trojan horse which allow questionable activity not always in the public interest, even though security agencies say it is. Who is going to challenge them if such activities are not subject to public scrutiny or effective oversight?

Some EU officials, alarmed by reports of the NSA's access to Internet companies, say Safe Harbor gives US companies a way to evade the EU's more stringent privacy regime.[677] European Parliament member Jan Philipp Albrecht told US officials in October 2013 that the agreement allows U.S companies to "circumvent" democratically established law. Albrecht said Europe "shouldn't allow our standards to be undermined by certain loopholes", which he said the Safe Harbor agreement facilitates.[678]

German federal data protection commissioner Peter Schaar called the Safe Harbor agreement a "fiction," given how much technology and the flow of information have changed in the past decade and how many new regulations Washington has drawn up since the treaty was signed. "Consequently, I do not think it is right that we continue to facilitate the transfer of data into the USA," Schaar said. The agreements "must be renegotiated, and must include reasonable protections against eavesdropping by state and secret services."[679]

In addition to their critique of Safe Harbor's lack of stringency, European regulators and others have attacked the agreement on the grounds that it is poorly enforced. EU officials released two reports critical of the program's enforcement in 2002 and 2004. Australian consulting firm Galexia reported hundreds of Safe Harbor violations in a 2008 report that criticised both the EU and the US for not taking enforcement more seriously. Indeed, the FTC did not bring its first enforcement under Safe Harbor rules until 2009, and its batch of seven enforcement actions that year targeted companies for falsely advertising their Safe Harbor certification, not for any failures to protect Europeans' data. Since then, the FTC has brought three Safe Harbor enforcement actions against Facebook, Google and MySpace.[680] Other testimony to the LIBE

[677] Mershon, Erin, "U.S. to EU: Don't scapegoat Safe Harbor over NSA", *Politico*, 7 Nov 2013. http://www.politico.com/story/2013/11/us-european-union-safe-harbor-nsa-99495.html?hp=l11

[678] Romm, Tony, and Erin Mershon, "EU to D.C.: Friends 'do not spy on each other'", *Politico*, 29 Oct 2013. http://www.politico.com/story/2013/10/european-union-nsa-friends-do-not-spy-on-each-other-99035.html

[679] Landler, Mark, and David E. Sanger, "Obama May Ban Spying on Heads of Allied States", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/obama-may-ban-spying-on-heads-of-allied-states.html?_r=0

[680] Mershon, Erin, "U.S. to EU: Don't scapegoat Safe Harbor over NSA", *Politico*, 7 Nov 2013. http://www.politico.com/story/2013/11/us-european-union-safe-harbor-nsa-99495.html?hp=l11

committee contends that "The Safe Harbor does not (and cannot) cover major categories of data that appear to be the subject of surveillance, including financial records, travel records, and significant portions of voice and data traffic carried by US telecommunications providers."[681]

In late November 2013, the European Commission released a Communication which was critical of the Safe Harbor Agreement, but did not completely sink it.[682] The Communication concludes that

> Due to deficiencies in transparency and enforcement of the arrangement, specific problems still persist and should be addressed:
> a) transparency of privacy policies of Safe Harbour members,
> b) effective application of Privacy Principles by companies in the US, and
> c) effectiveness of the enforcement.
> Furthermore, the large scale access by intelligence agencies to data transferred to the US by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data in transferred to the US.

The Commission makes 13 recommendations for improving the agreement. It says US authorities have until the summer of 2014 to implement the recommendations, at which point Commission will review the agreement and the actions taken by, inter alia, the FTC.

Circumventing laws

Some of the documents leaked by Snowden reveal how the intelligence agencies have attempted to circumvent or simply ignore laws that would limit the extent of their surveillance. According to a report in *The Guardian*, GCHQ was helping European partners to circumvent national laws.[683] "The files [leaked by Snowden] also make clear that GCHQ played a leading role in advising its European counterparts how to work around national laws intended to restrict the surveillance power of intelligence agencies."[684]

The Guardian claimed that it had obtained documents that show that GCHQ has had access to the PRISM system since at least June 2010. As a result, GCHQ might have been able to circumvent UK restrictions on accessing people's communications by

---

[681] Connolly, Chris (Galexia), EU/US Safe Harbour – Effectiveness of the Framework in relation to National Security Surveillance, Speaking/background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) Inquiry on "Electronic mass surveillance of EUY citizens", Strasbourg, 7 Oct 2013, pp. 2, 6. http://www.europarl.europa.eu/committees/en/libe/events.html#menuzone

[682] European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847, Brussels, 27 Nov 2013. http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

[683] Deutsche Welle, "Germany admits Europe's spy agencies cooperate on surveillance", 2 Nov 2013. http://www.dw.de/germany-admits-europes-spy-agencies-cooperate-on-surveillance/a-17200903

[684] Borger, Julian, "GCHQ and European spy agencies worked together on mass surveillance", *The Guardian*, 1 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

obtaining the information from the NSA instead.[685] David Cameron has rejected allegation that GCHQ acted illegally by receiving information from the US.[686]

Some intelligence agencies have not had to circumvent national legislation because they have already been given a free hand. Such is the case in Sweden which passed a law in 2008 allowing its intelligence agency to monitor cross-border e-mail and phone communications without a court order.[687]

Unlawful access to SWIFT?

The Dutch and Belgian data protection authorities are leading an investigation into whether the SWIFT payment network is safe, following media reports that the NSA has or has had unlawful access to SWIFT data concerning international bank transfers. In October 2013, SWIFT said it had conducted an audit that showed that nothing wrong had happened. The European Parliament, however, demanded a halt to bank-data transfers to US counter-terrorism investigators because of possible data protection violations. The Article 29 Data Protection Working Party agreed that Belgium and the Netherlands should lead the investigation because SWIFT is based in Belgium and has an important data processing centre in the Netherlands.[688]

Brazil and German resolution to UN

Brazil and Germany formally presented a resolution on "The right to privacy in the digital age" to the UN General Assembly on 1 November 2013 urging all countries to extend internationally guaranteed rights to privacy to the Internet and other electronic communications.[689]

The draft resolution

> 1. Reaffirms the rights contained in the International Covenant on Civil and Political Rights, in particular the right to privacy and not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, and the right to enjoy protection of the law against such interference or attacks, in accordance with article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights;

It calls upon States

---

[685] Hope, Christopher, and Tom Whitehead, "British Intelligence watchdog flies to Washington to demand answers on snooping scandal", *The Telegraph*, 7 June 2013. http://www.telegraph.co.uk/technology/internet-security/10107059/British-Intelligence-watchdog-flies-to-Washington-to-demand-answers-on-snooping-scandal.html

[686] Warrell, Helen, and James Blitz, "David Cameron rejects claims GCHQ broke law over US Prism data", *The Financial Times*, 10 June 2013. http://www.ft.com/cms/s/0/01d745fe-d1f0-11e2-b17e-00144feab7de.html#axzz2VsHkbdAE

[687] Borger, Julian, "GCHQ and European spy agencies worked together on mass surveillance", *The Guardian*, 1 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

[688] Bodoni, Stephanie, "Global Data Network Probed by EU Regulators Over NSA Reports", *Bloomberg News*, 13 Nov 2013. http://www.bloomberg.com/news/2013-11-13/global-data-network-probed-by-eu-regulators-over-nsa-reports.html

[689] A copy of the resolution can be found at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45

> 4 (b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law
>
> 4 (d) To establish independent national oversight mechanisms capable of ensuring transparency and accountability of State surveillance of communications, their interception and collection of personal data;

It also

> 5. Requests the United Nations High Commissioner for Human Rights to submit an interim report on the protection of the right to privacy in the context of domestic and extraterritorial surveillance of communications, their interception and collection of personal data, including massive surveillance, interception and collection of personal data, to the General Assembly at its sixty-ninth session.

Although General Assembly resolutions are not legally binding, they do reflect world opinion and carry moral and political weight.[690] The 4(d) provision above is especially interesting in view of one of the conclusions we draw in this paper, i.e., the failure of existing oversight mechanisms.

Meanwhile, in advance of adoption of the resolution, the Frankfurter Allgemeine Sonntagszeitung (FAS) reported on 2 November 2013 that Germany and the US had struck an agreement not to spy on each other following discussions between a delegation of officials from Merkel's office and German intelligence officials and officials at the White House.[691]

In late November 2013, the UN General Assembly's human rights committee unanimously adopted the resolution. The United States did not oppose it, but lobbied successfully to water it down somewhat by dropping a key provision stating that the domestic and international interception and collection of communications and personal data, "in particular massive surveillance", may constitute a human rights violation.[692]

Study finds mass surveillance violates EU law

While the intelligence agencies and political leaders said that the surveillance conducted was within the law, the media, academics and advocacy organisations have disputed those claims. A study presented by Sergio Carrera of the Centre for European Policy Studies (CEPS) and Francesco Ragazi of Leiden University shows that mass Internet surveillance by US and UK intelligence agencies violates EU law. The authors presented their findings to the European Parliament's LIBE Committee

---

[690] The Associated Press, "Internet privacy resolution presented to United Nations", published in the *Portland Press Herald*, 8 Nov 2013.
http://www.pressherald.com/news/nationworld/Internet_privacy_resolution_presented_to_United_Nations_.html

[691] *Deutsche Welle*, "Germany admits Europe's spy agencies cooperate on surveillance", 2 Nov 2013.
http://www.dw.de/germany-admits-europes-spy-agencies-cooperate-on-surveillance/a-17200903

[692] Spielmann, Peter James, "UN advances Internet privacy resolution", Associated Press, published in *The Miama Herald*, 26 Nov 2013. http://www.miamiherald.com/2013/11/26/3780690/un-advances-internet-privacy-rights.html

on Civil Liberties, Justice and Home Affairs.[693] Carrera and Ragazi are not alone. Others also believe that, with few exceptions, NSA spying on the EU and the UN "not only contravenes the diplomatic code, but also international agreements. The Convention on the Privileges and Immunities of the United Nations of 1946, as well as the Vienna Convention on Diplomatic Relations of 1961, long ago established that no espionage methods are to be used. What's more, the US and the UN signed an agreement in 1947 that rules out all undercover operations."[694]

Months before the Carrera and Ragazi presentation, in fact, within days of the first revelations, the Council of Europe alerted its 47 member states to the risks of digital tracking and other surveillance technologies for human rights, the rule of law and democracy, and recalled the need to ensure their legitimate use. In a Declaration issued to governments, the Committee of Ministers said that legislation allowing for overly broad surveillance of citizens can challenge their privacy and have a chilling effect on their freedom of expression and the freedom of the media. The Committee said that tracking and surveillance measures by law enforcement authorities should comply with the Council of Europe's human rights standards set out in the European Convention on Human Rights. Such measures should also strictly respect the limits, requirements and safeguards set out in the Data Protection Convention 108. The Declaration drew attention to the criminal law implications of unlawful surveillance and tracking and to the relevance of the Budapest Convention on Cybercrime.[695]

Societal response

Gore: Blanket surveillance is obscenely outrageous

The societal response can be judged by, inter alia, comments from members of the public in response to news stories and public opinion surveys.
Here is an example of a comment:

> How is spying on the leaders of allied nations useful in fighting terrorism? How did it save lives? So the leaders of France, Germany, Italy, Spain, etc should all thank us for our intrusive, abrasive, and illegal acts, is that right? Have the leaders of the American government gone completely mad?[696]

---

[693] Ashford, Warwick, "NSA and GCHQ mass surveillance violates EU law, study finds", *ComputerWeekly.com*, 8 Nov 2013. http://www.computerweekly.com/news/2240208711/NSA-and-GCHQ-mass-surveillance-violates-EU-law-study-finds. The full study, by Bigo, Didier, Sergio Carrera, Nicholas Hernanz, et al., *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, October 2013, can be found here: http://www.europarl.europa.eu/committees/en/studies.html

[694] Poitras, Laura, "Marcel Rosenbach and Holger Stark, Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[695] Council of Europe, "Council of Europe alerts governments on risks of digital tracking and surveillance", Press release, DC 081(2013), Strasbourg, 12 June 2013. http://hub.coe.int/web/coe-portal/press/pressreleases

[696] From crygdyllyn, 29 Oct 2013:http://www.politico.com/gallery/2013/10/nsa-spying-15-great-quotes/001396-019790.html

This comment has been echoed by other stakeholders. Former Vice President Al Gore tweeted that privacy is essential in the digital era: "Is it just me, or is secret blanket surveillance obscenely outrageous?"[697]

Anthony Romero of the American Civil Liberties Union denounced the surveillance as an infringement of fundamental individual liberties. "A pox on all the three houses of government," Mr. Romero said. "On Congress, for legislating such powers, on the FISA court for being such a paper tiger and rubber stamp, and on the Obama administration for not being true to its values."[698]

Democratic Senator Ron Wyden of Oregon said he hoped the disclosure would "force a real debate" about whether such "sweeping, dragnet surveillance" should be permitted — or is even effective. The UK's Lord Ashdown has said that surveillance should only be conducted against specific targets when there was evidence against them and that dragnet surveillance was unacceptable.[699]

Moreover, Lord Ashdown has said it was time for a high-level inquiry to address fundamental questions about privacy in the 21st century, and railed against "lazy politicians" who frighten people into thinking "al-Qaida is about to jump out from behind every bush and therefore it is legitimate to forget about civil liberties…Well it isn't."

Various other public figures have commented on the surveillance revelations. For example, World Wide Web creator Sir Tim Berners-Lee has warned that the democratic nature of the Internet is threatened by a "growing tide of surveillance and censorship".[700]

Public opinion surveys

There have been various surveys of the public's views of the massive surveillance since the NSA revelations began, especially in the US.

A Pew Research Center survey taken there a few days after the leaks found that a majority of respondents (56%) believed that monitoring their phone calls was an "acceptable" way to investigate terrorism, though a substantial minority (41%) disagreed. On the question of e-mail monitoring, the split went the other way: 52% said it was unacceptable while 45% approved. Interestingly, 62% said it was more important for the federal government to investigate possible terrorist threats, even if that intrudes on personal privacy. Just 34% said it was more important for the

---

[697] Associated Press, "Obama administration collecting huge number of citizens' phone records, lawmaker says", 6 June 2013. http://www.washingtonpost.com/politics/federal_government/report-government-secretly-scooping-up-phone-records-of-millions-of-verizon-customers/2013/06/05/e820deb8-ce57-11e2-8573-3baeea6a2647_story.html

[698] Savage, Charlie, Edward Wyatt and Peter Baker, "U.S. Says It Gathers Online Data Abroad", *The New York Times*, 6 June 2013. http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?hp&_r=1&

[699] Nick Hopkins and Matthew Taylor, "Surveillance technology out of control, says Lord Ashdown", *The Guardian*, 18 Nov 2013. http://www.theguardian.com/world/2013/nov/18/surveillance-technology-out-of-control-ashdown

[700] BBC News, "Tim Berners-Lee says 'surveillance threatens web'", 22 Nov 2013. http://www.bbc.co.uk/news/technology-25033577

government not to intrude on personal privacy, even if that limits its ability to investigate possible terrorist threats.[701]

In a mid-July Washington Post-ABC News survey, nearly half (49 per cent) said they thought that the NSA's surveillance program intruded on their personal privacy rights. And 74 per cent said it infringed on some Americans' privacy, if not their own. Nevertheless, when asked to balance security worries against privacy concerns, Americans continued to opt for security. In that same Washington Post-ABC News poll, 57 per cent felt that it was important for the federal government to investigate terrorist threats, even if it intrudes on personal privacy. Just 39 per cent said that the government should not intrude on personal privacy, even if it limits the ability to investigate possible terrorist threats.[702]

A Pew Research poll in July 2013 found that a majority of Americans – 56% – said that federal courts fail to provide adequate limits on the telephone and Internet data the government is collecting as part of its anti-terrorism efforts. An even larger percentage (70%) believed that the government has been using this data for purposes other than investigating terrorism. And despite the insistence by the president and other senior officials that only "metadata", such as phone numbers and e-mail addresses, were being collected, 63% thought the government was also gathering information about the content of communications – with 27% believing the government has listened to or read their phone calls and e-mails.[703]

In another poll in July, Annalect, a US data analytics company, found that the percentage of Internet users worried about their online privacy jumped 19 per cent, from 48 per cent in June (when the NSA revelation stories first appeared in *The Guardian* and *The Washington Post*) to 57 per cent in July. When consumers were asked about their response to the NSA's collection of online information, nearly one-third (31 per cent) said they were now taking action to protect their online privacy, such as changing their browser settings, deleting or opting out of mobile tracking, disabling cookies and editing social media profiles.[704]

A majority of Americans oppose the NSA's collection of data on telephone and Internet usage, according to a poll conducted by the Associated Press-NORC Center for Public Affairs Research in August 2013, following more than two months of disclosures about the NSA's mass surveillance programs. The poll showed that a majority of Americans believed the US government was doing a poor job of protecting privacy rights, that 71 per cent did not want officials eavesdropping on US

---

[701] Pew Research Center, "Public Says Investigate Terrorism, Even If It Intrudes on Privacy", 10 June 2013.
http://www.people-press.org/files/legacy-pdf/06-10-13%20PRC%20WP%20Surveillance%20Release.pdf

[702] Stokes, Bruce, "Trading Privacy for Security", *Foreign Policy*, 4 Nov 2013.
http://www.foreignpolicy.com/articles/2013/11/04/trading_privacy_for_security?wp_login_redirect=0

[703] Pew Research Center for the People & the Press, "Few See Adequate Limits on NSA Surveillance Program", 26 July 2013. http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/

[704] Bachman, Katy, "Study: NSA Scandal Is Still Setting Off Privacy Alarm Bells Among Consumers", *AdWeek*, 13 Aug 2013. http://www.adweek.com/news/technology/study-nsa-scandal-still-setting-privacy-alarm-bells-among-consumers-151835

phone calls without court warrants while 62 per cent opposed collection of the contents of Americans' e-mails without warrants.[705]

Another survey, the results of which were published by the Pew Research Center in November 2013, found that 56 per cent of Americans thought it was unacceptable for the United States to monitor the phone calls of the leaders of allied nations, including German Chancellor Angela Merkel.[706]

An October 2013 survey of American, Canadian and British adults by Angus Reid Global indicated that people distrust their national leaders to be good guardians of the information gathered or to restrict its use to national security purposes. When asked whether they trusted their national government to be "a good guardian of citizens' personal information", 60 per cent of Americans and 64 per cent of Britons and Canadians said they had "not that much trust" or "no trust at all". In each country polled, at least 75 per cent of respondents described the issue of government surveillance of the public's Internet communications as "very" or "quite" important to them (US: 77%, Canada: 78% UK: 82%). Asked to assume their national government is routinely conducting electronic surveillance of the general public, 60% of Americans and Canadians described this as "unacceptable", while Britons were more split, (52% unacceptable versus 48% acceptable). Only one in five respondents believe information gathered by governments will be used for "strictly national security/anti-terrorism efforts" (US: 21%, UK: 19%, Canada: 18%).

The NSA revelations seem to have had a salutary effect on the public's paying more attention to their privacy. A Harris poll released 13 November 2013 showed that four out of five people have changed the privacy settings of their social media accounts, and most have made changes in the previous six months.[707]

Interestingly, public opinion in the UK does not seem to be so opposed to what the intelligence agencies have been doing. According to a YouGov poll in September 2013, only 19% of the public think that the British security services should cut back their surveillance powers – and they tend to believe recent leaks about them are a bad thing. While there has also been widespread distress over the content of the leaks, YouGov found little public support for scaling back the surveillance state. Only 19% of British adults say the British security services have too many powers. The largest group, 42%, say the current balance is about right, and 22% say they do not have enough powers.[708]

Snowden: hero or traitor?

---

[705] Associated Press, "Poll: American public's concerns rise over surveillance programs and privacy erosion", 10 Sept 2013. http://www.foxnews.com/us/2013/09/10/poll-american-public-concerns-rise-over-surveillance-programs-and-privacy/

[706] Pew Research Center, "Most Say Monitoring Allied Leaders' Calls Is Unacceptable", 4 Nov 2013. http://www.people-press.org/2013/11/04/most-say-monitoring-allied-leaders-calls-is-unacceptable/

[707] Acohido, Byron, "Snowden effect: young people now care about privacy", *USA Today*, 13 Nov 2013. http://www.usatoday.com/story/cybertruth/2013/11/13/snowden-effect-young-people-now-care-about-privacy/3517919/

[708] Dahlgreen, Will, "Little appetite for scaling back surveillance", YouGov, 13 Oct 2013. http://yougov.co.uk/news/2013/10/13/little-appetite-scaling-back-surveillance/

Former US Vice President Dick Cheney has called Snowden a "traitor" for leaking NSA documents.[709] While Cheney and other US government officials have said Snowden should be captured and punished, others regard Snowden as a hero. Edward Snowden has been likened to Daniel Ellsberg, the man who in 1971 leaked the Pentagon Papers to *The New York Times*, which revealed that the US government had been less than truthful with the public about the conduct of the Vietnam war. The Pentagon Papers came as a shock to the public, and to lawmakers. Ellsberg, like Snowden, was initially accused of espionage and conspiracy, though those charges were ultimately dropped. Today, he is mostly seen as a hero of open government and free speech.[710] According to the Angus Reid Global online poll, 51 per cent of Americans viewed Snowden as a hero, and 49 per cent as a traitor.[711] However, in Canada, 67% and in the UK, 60% of respondents say Snowden should be commended for his actions. In a separate survey conducted by public broadcaster ARD and *Die Welt*, 60 per cent of Germans regard Snowden as a hero. Meanwhile, Germans' trust in the US has plummeted from 76 per cent when Obama made his first official visit to Berlin in November 2009 to only 35 per cent four years later, in November 2013.[712]

The Council of Europe issued a press release saying "'Whistleblowers' who disclose state wrongdoing in the public interest should be protected from retaliation, provided they acted in good faith and followed procedures, a committee of the Parliamentary Assembly of the Council of Europe (PACE) said in a draft resolution" in June. While the press release didn't mention Snowden by name, the message was clear enough.[713] As it turns out, a pro-Snowden petition on the White House website garnered more than 100,000 supporters within three weeks of the initial leaks.[714]

One of the first to call Snowden a hero was film-maker Oliver Stone who hailed Snowden as a hero for exposing the NSA's mass surveillance programme. "It's a disgrace that Obama is more concerned with hunting down Snowden than reforming these George Bush-style eavesdropping techniques," the Oscar-winning director told audiences at an international film festival in the Czech Republic in early July 2013.[715] Another public figure of note to describe Snowden as a hero is James Wales, founder of Wikipedia. Wales said of Snowden that "he has never leaked anything that would put any particular agents at risk and so forth. He has exposed what I believe to be, very likely to be judged, criminal wrongdoing, lying to Congress and certainly a

---

[709] Rhodan, Maya, "Dick Cheney Calls Snowden a 'Traitor,' Defends NSA", *Time*, 28 Oct. 2013. http://swampland.time.com/2013/10/28/dick-cheney-calls-snowden-a-traitor-defends-nsa/

[710] *The Globe and Mail*, "Is Edward Snowden a hero?", Globe editorial, 8 Nov 2013. http://www.theglobeandmail.com/globe-debate/editorials/is-edward-snowden-a-hero/article15354202/

[711] Raphael, Daniel, "Why Edward Snowden Is a Hero", *Huffington Post*, 7 Nov 2013. http://www.huffingtonpost.com/daniel-raphael/why-edward-snowden-is-a-h_b_4227605.html

[712] RT, "Germans lose trust in US, see NSA whistleblower Snowden as hero – poll", 8 Nov 2013. http://rt.com/news/germany-lose-trust-us-snowden-431/

[713] Council of Europe, "PACE committee calls for protection of 'whistleblowers' who reveal state wrongdoing", Press release, AP117 (2013), Strasbourg, 24 June 2013. http://hub.coe.int/web/coe-portal/press/pressreleases

[714] Nelson, Steven, "White House Says It Will Respond to 'Pardon Edward Snowden' Petition", *U.S. News & World Report*, 25 Nov 2013. http://www.usnews.com/news/articles/2013/11/25/white-house-says-it-will-respond-to-pardon-edward-snowden-petition

[715] Brooks, Xan, "Oliver Stone defends Edward Snowden over NSA revelations", *The Guardian*, 5 July 2013. http://www.guardian.co.uk/film/2013/jul/05/oliver-stone-edward-snowden-nsa

shock and an affront, in America, an affront to the 4th amendment. I think that history will judge him very favourably."[716]

In an editorial, Canada's national newspaper, *The Globe and Mail*, argued that Snowden has performed a service to the public. The editorial noted, "There's is no perfect balance that can ever be struck between privacy and national security. In a post-9/11 world, the arguments of national security were often treated as irresistible, and impossible to counter. Mr. Snowden's revelations have altered the debate, and for the better."[717]

Venezuelan President Nicolás Maduro similarly said Snowden should be given a "humanitarian medal" for revealing details of NSA surveillance programmes on US and foreign citizens. "He did not kill anyone and did not plant a bomb…. What he did was tell a great truth in an effort to prevent wars. He deserves protection under international and humanitarian law."[718]

Stephen Walt, a professor of international affairs at Harvard University, writing in *The Financial Times*, made similar comments. "Mr Snowden's motives were laudable: he believed fellow citizens should know their government was conducting a secret surveillance programme enormous in scope, poorly supervised and possibly unconstitutional. He was right." Walt argued that Snowden deserves a presidential pardon. "Gerald Ford pardoned Richard Nixon, George HW Bush pardoned the officials who conducted the illegal Iran-Contra affair, and Mr Obama has already pardoned several convicted embezzlers and drug dealers. Surely Mr Snowden is as deserving of mercy as these miscreants."[719]

For its part, *The New York Times*, which broke many of the stories about NSA abuse, has said that Snowden "has done his country a great service. It is time for the United States to offer Mr. Snowden a plea bargain or some form of clemency… When someone reveals that government officials have routinely and deliberately broken the law, that person should not face life in prison at the hands of the same government."[720]

Applying pressure on countries, Snowden and journalists

After Ecuador withdrew its offer of asylum to Snowden, a US state department spokeswoman denied the US had bullied other potential host countries. She said that

---

[716] Al Jazeera, "Wikipedia founder calls Edward Snowden a hero", 25 Nov 2013. http://www.aljazeera.com/pressoffice/2013/11/wikipedia-founder-calls-edward-snowden-hero-20131125142412647981.html

[717] *The Globe and Mail*, "Is Edward Snowden a hero?", Globe editorial, 8 Nov 2013. http://www.theglobeandmail.com/globe-debate/editorials/is-edward-snowden-a-hero/article15354202/

[718] Roberts, Dan, "Bolivian president's jet rerouted amid suspicions Edward Snowden on board", *The Guardian*, 3 July 2013. http://www.theguardian.com/world/2013/jul/03/edward-snowden-bolivia-plane-vienna

[719] Walt, Stephen, "Snowden deserves an immediate presidential pardon", *The Financial Times*, 8 July 2013. http://www.ft.com/cms/s/0/0ccf2d14-e7c1-11e2-babb-00144feabdc0.html#axzz2YiI70RAU

[720] The Editorial Board, "Edward Snowden, Whistle-Blower", *The New York Times*, 1 Jan 2014. http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?hp&rref=opinion&_r=0

the US has simply impressed upon possible host countries the seriousness of the crimes with which Snowden has been charged.[721]

Some politicians favour prosecuting the newspapers publishing the reports based on the documents leaked by Snowden. In the UK, Tory MP Julian Smith said the newspaper had broken the law and should be prosecuted. The backbencher reportedly made a complaint about *The Guardian* to the police, and criticised the newspaper for writing stories "with no consultation with government". Home Office minister James Brokenshire said that *The Guardian*'s publication of the Snowden leaks had damaged national security.[722]

Some of the journalists who brought the NSA documents leaked by Snowden to light have been isolated or harried by the US and UK governments. Sarah Harrison, the British journalist and WikiLeaks staffer who had been working with Snowden since his arrival in Moscow, eventually left Russia (in November 2013) and joined other activists in Berlin. Her lawyers reportedly advised her that it was "not safe to return home" to the UK. Harrison joined other journalists and activists who were involved in the publication of Snowden's files and are now living in the German capital "in effective exile", including Laura Poitras and Jacob Applebaum.[723]

Economic response

Many people think the NSA surveillance practices have not only been aimed at intercepting communications by terrorists, but also aimed at helping US industry. US Director of National Intelligence James Clapper has said the US does not use its foreign intelligence capabilities "to steal the trade secrets of foreign companies on behalf of US companies to enhance their international competitiveness or increase their bottom line." But leaked documents showing that the NSA spied on Brazilian oil company Petrobras and gained access to data held by US cloud providers including Google and Yahoo indicate otherwise.[724] The fact that the US Trade Representative asked the NSA to collect data on organisations also suggests the NSA's surveillance capabilities were used in order to further US trade policies.[725] Other leaked documents purportedly show that the NSA and GCHQ both spied on OPEC.[726] A former US Vice

---

[721] Roberts, Dan, "Bolivian president's jet rerouted amid suspicions Edward Snowden on board", *The Guardian*, 3 July 2013. http://www.theguardian.com/world/2013/jul/03/edward-snowden-bolivia-plane-vienna

[722] Mason, Rowena, "Edward Snowden NSA files: Guardian should be prosecuted, says Tory MP", *The Guardian*, 22 Oct 2013. http://www.theguardian.com/politics/2013/oct/22/edward-snowden-guardian-should-be-prosecuted-tory-mp

[723] Oltermann, Philip, "Sarah Harrison joins other Edward Snowden files 'exiles' in Berlin", *The Guardian*, 6 Nov 2013. http://www.theguardian.com/world/2013/nov/06/sarah-harrison-edward-snowden-berlin

[724] Bryant, Chris, "NSA revelations boost corporate paranoia about state surveillance", *The Financial Times*, 31 Oct 2013. http://www.ft.com/intl/cms/s/0/ec02a8ca-422b-11e3-bb85-00144feabdc0.html

[725] Shane, Scott, "No Morsel Too Minuscule for All-Consuming N.S.A.", *The New York Times*, 2 Nov 2013.
http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?src=un&feedurl=http%3A%2F%2Fjson8.nytimes.com%2Fpages%2Fworld%2Feurope%2Findex.jsonpThe same story says the NSA's "official mission list includes using its surveillance powers to achieve… 'economic advantage' over Japan and Brazil, among other countries".

[726] Spiegel Online International, "Oil Espionage: How the NSA and GCHQ Spied on OPEC", 11 Nov 2013. http://www.spiegel.de/international/world/how-the-nsa-and-gchq-spied-on-opec-a-932777.html

President has said that the US intelligence capability "is enormously important to the United States, to our conduct of foreign policy, to the defense matters, to *economic matters*"[727] [Italics added.] – which further suggests that the NSA's surveillance activities are not only directed towards countering terrorism, but giving the US and American companies economic leverage and insight into the negotiating strategies of other countries and companies.

Further evidence of the NSA and GCHQ having economic targets is evident in reports of leaked documents in December 2013 indicating that European Commission Trade Commissioner Joaquín Almunia was a target of their surveillance. *The Guardian* pointed out that Almunia is in charge of major anti-monopoly investigations and approving mergers of companies with significant presence in the EU. He has been involved in a long-running investigation into Google over complaints about the company's alleged stranglehold on online advertising. He has also clashed with Google and Microsoft over privacy concerns.[728] The same report said that French defence and logistics giant Thales Group, part-owned by the French government, was also a target.

NSA revelations threatened EU-US trade agreement

There were concerns that the surveillance revelations would complicate negotiations on a wide-ranging free trade agreement between Europe and the United States.[729] Some politicians said the free trade negotiations should be put on hold. European Commission Vice-President Viviane Reding stated, "We cannot negotiate on a large trans-Atlantic market if there is the slightest suspicion that our partners are spying on the offices of our chief negotiator."[730]

Nevertheless, the trade talks on the so-called Transatlantic Trade and Investment Partnership (TTIP) resumed in early November 2013. Some have estimated that a deal could bring annual benefits of €119 billion for the 28 EU Member States. Personal data protection still remains a potential stumbling block. An EU official close to the trade talks conceded "there may be issues of trust", but stressed that Europe would not compromise its personal data protection standards even as it must discuss the wider issue of information transfer.[731]

---

[727] Rhodan, Maya, "Dick Cheney Calls Snowden a 'Traitor,' Defends NSA", *Time*, 28 Oct. 2013. http://swampland.time.com/2013/10/28/dick-cheney-calls-snowden-a-traitor-defends-nsa/

[728] Ball, James, and Nick Hopkins, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief", *The Guardian*, 20 Dec 2013. http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

[729] Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html

[730] Poitras, Laura, Marcel Rosenbach and Holger Stark, "Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[731] AFP, "EU, US return to trade talks under spy scandal cloud", published in *The Nation*, 12 Nov 2013.
http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/international/12-Nov-2013/eu-us-return-to-trade-talks-under-spy-scandal-cloud

Storms in the cloud

The European Parliament commissioned a report in 2012 that revealed that the EU was failing to protect its citizens from US surveillance. The October 2012 report warned the European Parliament that the FISA law had granted American spies "heavy-calibre mass-surveillance firepower" and recommended that cloud-storage providers should be required to warn European users of the risks.[732]
The Information Technology and Innovation Foundation, a non-partisan research and advocacy group funded in part by the technology industry published a report in August 2013 estimating that US data cloud providers could lose $21.5 billion to $35 billion in business over the next three years as a result of the revelations.[733] Some US companies have said they have already lost business, while UK rivals have said that UK and European businesses are increasingly wary of trusting their data to American organisations, which might have to turn it over secretly to the NSA.[734]

A survey by the US-based Cloud Security Alliance found that of those outside the US, 10% had cancelled a project with a US-based cloud computing provider, and 56% would be "less likely" to use a US-based cloud computing service.[735] European officials have also talked about the need to have stronger cloud computing capabilities in Europe to provide stronger privacy protections for citizens.[736]

Similar but more specific findings came from a survey conducted by a Vancouver-based web hosting company, Peer 1 Hosting which polled 300 UK and Canadian businesses and found 25 per cent were taking steps to move data storage outside of the US as a result of privacy scandals. Meanwhile, 96 per cent considered security and 82 per cent considered data privacy their top concerns.[737]

NSA surveillance has already caused considerable political damage in the case of Brazil, seriously undermining the trust between Rousseff and Obama. Brazil now plans to introduce a law that will force companies such as Google and Facebook to store their data inside Brazil's borders, rather than on servers in the US, making these

---

[732] *The Economist*, "Surveillance: Look who's listening", 15 June 2013. http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[733] Birnbaum, Michael, "Germany looks at keeping its Internet, e-mail traffic inside its borders", *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

[734] Arthur, Charles, "Fears over NSA surveillance revelations endanger US cloud computing industry", *The Guardian*, 8 Aug 2013. http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing. See also Stern-Peltz,, Mikkel, and Jim Armitage, "IT firms lose billions after NSA scandal exposed by whistleblower Edward Snowden", *The Independent*, 29 Dec 2013. http://www.independent.co.uk/life-style/gadgets-and-tech/news/it-firms-lose-billions-after-nsa-scandal-exposed-by-whistleblower-edward-snowden-9028599.html

[735] Arthur, Charles, "Fears over NSA surveillance revelations endanger US cloud computing industry", *The Guardian*, 8 Aug 2013. http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing

[736] Dyer, Geoff, and Richard Waters, "Spying revelations will speed fragmentation of internet, say experts", *The Financial Times*, 31 Oct 2013. http://www.ft.com/cms/s/0/e028f49c-4257-11e3-9d3c-00144feabdc0.html#axzz2jMUcr8o3

[737] Acohido, Byron, "Snowden affair continues to chill cloud spending", *USA Today*, 8 Jan 2014. http://www.usatoday.com/story/cybertruth/2014/01/08/snowden-affair-continues-to--chill-cloud-spending/4360977/

international companies subject to Brazilian data privacy laws. The Brazilian government is also developing a new encryption system to protect its own data against hacking.[738]

European 'clouds'

Some German companies have seen the Snowden revelations as a marketing opportunity – by offering German customers services that keep German e-mail and Internet traffic within German borders. The companies claim they can improve the security of German communications as they are subject to stricter privacy regulations than the US.[739] The German initiative somewhat mimics that of Brazil whose president, Dilma Rousseff, was also allegedly monitored by the NSA.[740]

European Union leaders have advocated that their 28 nations develop "cloud" data storage that is independent from the United States.[741] Out-Law.com notes that businesses should evaluate their data storage and outsourcing contracts in light of the recent NSA disclosures. "The news could have major implications for outsourcing," the report states, "and will have been unsettling reading for many companies which use cloud services."[742]

Such talk may be one reason why some US industry representatives have reacted angrily to the Snowden revelations. Google Executive Chairman Eric Schmidt, for example, said it was "outrageous", if reports were correct, that the NSA intercepted the company's data centres, especially without authorisation.[743]

Better encryption versus targeted adverts

Standards organisations and many companies are reviewing their encryption practices to see how they can make their communications more secure. Google, Yahoo, Twitter and others are doing likewise, but the snag for such companies is that when

---

[738] Glüsing, Jens, Laura Poitras, Marcel Rosenbach and Holger Stark, "Fresh Leak on US Spying: NSA Accessed Mexican President's Email", *Spiegel Online International*, 20 Oct 2013. http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

[739] Birnbaum, Michael, "Germany looks at keeping its Internet, e-mail traffic inside its borders", *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

[740] Birnbaum, Michael, "Germany looks at keeping its Internet, e-mail traffic inside its borders", *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

[741] Birnbaum, Michael, "Germany looks at keeping its Internet, e-mail traffic inside its borders", *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

[742] Bracy, Jedidiah, "NSA Leaks: EU-U.S. Tensions on the Rise, Europe Reacts", *The Privacy Advisor*, IAPP. International Association of Privacy Professionals, 13 June 2013. https://www.privacyassociation.org/publications/nsa_leaks_eu_u.s._tensions_on_the_rise_europe_reacts_roundup

[743] Kan, Deborah, "Google Chairman Lambastes NSA Actions as 'Outrageous'", *The Wall Street Journal*, 4 Nov. 2013. http://online.wsj.com/news/articles/SB10001424052702304391204579177104151435042

communications are encrypted and more secure, it makes it more difficult to monitor users' e-mails and to post adverts on them.[744]

The Internet Engineering Task Force (IETF) have asked the architects of Tor, networking software designed to make Web browsing private, to consider turning the technology into an Internet standard. The IETF is already working on encrypting more of the data that flows between the individual's computer and the websites visited.[745]

Lavabit refuses to be "complicit in crimes against the American people"

Not all US companies bowed to the demands of the US surveillance. Ladar Levison, the founder of Lavabit, the secure e-mail service used by Edward Snowden, shut down his service rather than be "complicit in crimes against the American people", as he put it. He shut down the service rather than comply with a court order to co-operate with the US government in surveillance of his customers. In shutting down his service, Levinson said he "would strongly recommend against anyone trusting their private data to a company with physical ties to the United States". Silent Circle, another provider of secure online services, announced that it too would shut down its own encrypted e-mail service, Silent Mail, rather than support government surveillance of its customers.[746]

Other economic impacts: Belgacom has to clean its computers of NSA spyware

The NSA's surveillance activities generated a variety of economic impacts and responses, not least of which is the cost for some organisations to clean their computers of NSA-installed malware, aimed at spying on high-interest individuals. A leaked document in November 2013 shows that the agency installed malware on some 50,000 computer networks, one of which was Belgacom, the Belgian telecom company.[747]

Media response

Not a one-day wonder

The phrase "one-day wonder" refers to an event that gets splashed across the front pages of newspapers, but the story only gets visibility for a day. The Snowden revelations about the extent of the NSA's surveillance have managed to hold the

---

[744] *The Economist*, "Internet security: Besieged", 9 Nov 2013. http://www.economist.com/news/science-and-technology/21589383-stung-revelations-ubiquitous-surveillance-and-compromised-software

[745] Talbot, David, "Group Thinks Anonymity Should Be Baked Into the Internet Itself", *MIT Technology Review*, 26 Nov 2013. http://www.technologyreview.com/news/521856/group-thinks-anonymity-should-be-baked-into-the-internet-itself/

[746] Ackerman, Spencer, "Lavabit email service abruptly shut down citing government interference", *The Guardian*, 9 Aug 2013. http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden

[747] Manning, Craig, "Report: NSA installed malware on 50,000 computer networks worldwide", *National Monitor*, 24 Nov 2013. http://natmonitor.com/2013/11/24/report-nsa-installed-malware-on-50000-computer-networks-worldwide/

media's attention for months since *The Guardian* broke the first story in early June 2013. That story made the front pages in various countries around the world, and the media have continued to give the Snowden revelations front-page treatment virtually every day since the first leaks appeared. Initially, the revelations appeared in *The Guardian*, *The New York Times* and *The Washington Post*, but since the early days of June, many newspapers have had "exclusives".

The Snowden revelations are arguably different from other leaks in the sense that the media have given them far more attention. The so-called "one-day wonder" does not apply to the revelations. Some newspapers say that Snowden passed on some 58,000 documents – and perhaps even more[748] – to the media, notably Glenn Greenwald of *The Guardian* and free-lancer Laura Poitras. Hence, the revelations could continue some time to come.

One could also argue that Snowden revelations have made headlines for such a long time because of a smart media strategy by *The Guardian* and others. They let out only bits and pieces and as soon as the media interest seems to be waning, they produce new stories, so that keeps the topic on the public agenda.

Austrian critic Karl Kraus has said a scandal begins when the police put an end to it, i.e., many people in the trade knew about the extent of surveillance, about the more or less secret co-operation of different security services worldwide, about the exchange of intelligence – but that was kept secret! Now such knowledge has become public, and that changes the rules of the game, since "secret service" has turned into a kind of "public service".

Political pressure on the media

One member of the US Congress has likened what journalists Laura Poitras and Glenn Greenwald have done to a form of treason, and they are well aware of the Obama administration's unprecedented pursuit of not just leakers but of journalists who receive the leaks.[749] The US and UK governments have put pressure on *The Guardian* and *The New York Times* to stop publishing stories based on the leaked documents suggesting that the media have threatened efforts to curtail terrorism.

Lord Carlile of Berriew, a leading QC and former terrorism watchdog in the UK, has described publication of stolen secrets by *The Guardian* as a "criminal act" and that it was wrong to paint the newspaper's journalists as "virtuous whistleblowers".[750]

---

[748] NSA director general Keith Alexander has been quoted as saying that "Snowden has shared somewhere between 50 and 200,000 documents with reporters". Mathew, Jerin, "Edward Snowden Leaked up to 200,000 NSA Top Secret Documents", *International Business Times*, 15 Nov 2013. http://www.ibtimes.co.uk/articles/522484/20131115/edward-snowden-nsa-scandal-keith-alexander.htm?utm_source=dlvr.it&utm_medium=gplus

[749] Maass, Peter, "How Laura Poitras Helped Snowden Spill His Secrets", *The New York Times*, 13 Aug 2013. http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?pagewanted=1&_r=0

[750] Barrett, David, "Publishing Edward Snowden security secrets a 'criminal' act, says former terrorism watchdog", *The Telegraph*, 24 Oct 2013. http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10401711/Publishing-Edward-Snowden-security-secrets-a-criminal-act-says-former-terrorism-watchdog.html

UK cabinet secretary Sir Jeremy Heywood told *The Guardian* to destroy the NSA files in its possession, apparently on instruction from Prime Minister David Cameron, as the files represented a threat to national security. *The Guardian* agreed to destroy two hard drives in the presence of two security experts from GCHQ after the government threatened to take legal action. *Guardian* editor Alan Rusbridger told officials that *The Guardian* would continue to report from the leaked documents because it had back-up copies in the US and in Brazil.[751]

David Cameron has said he would take stronger action against *The Guardian* and other newspapers to stop them from publishing stories about GCHQ surveillance.[752] *The Guardian*, he said, was refusing to behave with "social responsibility", despite repeated warnings that the revelations are damaging to national security.[753]

In early December 2013, *Guardian* editor Alan Rusbridger was summoned to give evidence at a parliamentary inquiry by the House of Commons Home Affairs Select Committee, where some MPs accused him of helping terrorists by making top secret information public and sharing it with other news organisations. One MP said Rusbridger had committed an offence under Section 58A of the Terrorism Act which says it is a crime to publish or communicate any information about members of the armed forces or intelligence services. At the same parliamentary inquiry, London Metropolitan Police Assistant Commissioner Cressida Dick told MPs the police were examining whether *Guardian* newspaper staff and David Miranda, partner of Glen Greenwald, should be investigated for terrorism offences over their handling of data leaked by Edward Snowden.[754]

The New York Times carried a trenchant editorial in support of *The Guardian* and decrying the challenge by the Cameron government to a free British press. *The Times* said in part:

> Unlike the United States, Britain has no constitutional guarantee of press freedom. Parliamentary committees and the police are now exploiting that lack of protection to harass, intimidate and possibly prosecute The Guardian… the public has a clear interest in learning about and debating the N.S.A.'s out-of-control spying on private communications. That interest is shared by the British public as well.

The Times attacks British parliamentarians for not asking tough questions of the British intelligence agencies and, instead, for going after *The Guardian*.

> Alan Rusbridger, the newspaper's editor, has been summoned to appear before a parliamentary committee next month to testify about The Guardian's internal editorial decision-making regarding the Snowden information. Members of Parliament have

---

[751] Watt, Nicholas, "Guardian told to destroy NSA files for national security, says Clegg", *The Guardian*, 21 Aug 2013. http://www.theguardian.com/uk-news/2013/aug/21/nsa-nick-clegg-guardian-leaked-files

[752] BBC News, "Cameron threatens to act against newspapers publishing security leaks", 28 Oct 2013. http://www.bbc.co.uk/news/uk-politics-24710826

[753] Shipman, Tim, "Prime Minister threatens Guardian with legal action over 'damaging' spy leaks", *Daily Mail*, 29 Oct 2013. http://www.dailymail.co.uk/news/article-2478692/Prime-Minister-threatens-Guardian-legal-action-damaging-spy-leaks.html

[754] James, William, and Michael Holden, "British news staff may face terrorism charges over Snowden leaks", Reuters, 3 Dec 2013. http://uk.reuters.com/article/2013/12/03/uk-britain-snowden-guardian-idUKBRE9B20TI20131203

> also demanded information on the newspaper's decision to make some of the leaked information available to other journalists, including those at The Times. That should be none of Parliament's business. Meanwhile, Scotland Yard detectives are pursuing a criminal investigation into The Guardian's actions surrounding the Snowden leaks.
>
> These alarming developments threaten the ability of British journalists to do their jobs effectively… The global debate now taking place about intelligence agencies collecting information on the phone calls, emails and Internet use of private citizens owes much to The Guardian's intrepid journalism. In a free society, the price for printing uncomfortable truths should not be parliamentary and criminal inquisition.

It is, principally, the media who stand between the Orwellian surveillance practices of government and big industry on the one hand and the public on the other. Governments, such as the UK's Cameron government, play a dangerous game with democracy by attacking the media's reportage of their abuses against the people.

Meanwhile, *The Guardian* cited remarks by Frank La Rue, the UN special rapporteur on freedom of expression, who said he was alarmed at the political reaction to the Snowden revelations. "I have been absolutely shocked about the way the Guardian has been treated, from the idea of prosecution to the fact that some members of parliament even called it treason," said La Rue. "I think that is unacceptable in a democratic society."[755]

The media remain defiant

In an editorial soon after the initial Snowden revelations, *The New York Times* commented in an editorial that

> the Obama administration issued the same platitude it has offered every time President Obama has been caught overreaching in the use of his powers: Terrorists are a real menace and you should just trust us to deal with them because we have internal mechanisms (that we are not going to tell you about) to make sure we do not violate your rights. Those reassurances have never been persuasive….[756]

Certainly such reassurances have not persuaded newspapers such as *The Guardian* which has continued to publish stories based on the revelations. Glenn Greenwald and his colleagues have remained defiant. "Exclusives" based on the leaked documents have now appeared in many newspapers, not only in the UK and US, but also in other countries, notably Germany, France, Spain, Brazil and elsewhere.

The media have been raising public awareness

Laura Poitras, one of the first three journalists to interview Snowden, commented about the NSA revelations: "Do I think the surveillance state is out of control? Yes, I do. This is scary, and people should be scared. A shadow and secret government has

---

[755] Matthew Taylor, Nick Hopkins and Phil Maynard, "UK's reputation is damaged by reaction to Edward Snowden, says UN official", *The Guardian*, 15 Nov 2013.
http://www.theguardian.com/world/2013/nov/15/uk-reputation-edward-snowden-un

[756] The Editorial Board, "President Obama's Dragnet", Editorial, *The New York Times*, 6 June 2013.
http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html?pagewanted=all&_r=

grown and grown, all in the name of national security and without the oversight or national debate that one would think a democracy would have."[757]

The media have played an enormous role in raising citizen awareness of the surveillance revelations and its consequences. The reportage has had a strongly ripple effect throughout society as civil society activists have mobilised against dragnet surveillance and other public figures have lent their support to attempt to rein back the extent to which the NSA and others are able conduct their activities with little effective oversight and massive budgets.

Positive impacts of the revelations

The Snowden revelations have immeasurably helped to raise society's awareness of the pervasiveness of surveillance by the NSA and, to a lesser extent, GCHQ and other intelligence agencies. The revelations may also have increased public attention to the ubiquity of surveillance more generally, including that by large corporations.

The revelations have placed surveillance high on the political agenda. The issue of accountability is being discussed. Until the revelations began, it appeared that there was minimal or no accountability of the NSA and GCHQ to their elected officials.

Awareness of the extent of surveillance by the NSA and GCHQ has led to resistance, i.e., some politicians, such as Angela Merkel, have called for the NSA to stop monitoring their mobile phone calls. Brazilian president Dilma Rousseff showed her anger at NSA monitoring her communications by cancelling a meeting with Obama and by promoting legislation to force global Internet companies to store data obtained from Brazilian users inside the country.[758] Some of the companies subject to surveillance intrusions have increased their security to make it more difficult for governments to surveil their networks.[759]

The revelation that the NSA has been monitoring not only the communications of ordinary citizens but also the political leaders of 35 ally countries has led to greater solidarity between the political leaders and citizens. Angela Merkel did not say much when the NSA's monitoring of Germans was made public, but she was much more forthright when she learned that the NSA had been monitoring her calls since 2002. At first, when the revelations began, Merkel defended German co-operation with the NSA. "The work of intelligence agencies in democratic states was always vital to the safety of citizens and will remain so in the future," Ms. Merkel was quoted as saying in an interview published in the newspaper *Die Zei*t. "For me, there is absolutely no comparison between the Stasi in East Germany and the work of intelligence services in democratic states," she added, calling the programs "two totally different things." In the *Die Zeit* interview, Ms. Merkel reminded Germans of the important role the

[757] Maass, Peter, "How Laura Poitras Helped Snowden Spill His Secrets", *The New York Times*, 13 Aug 2013. http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?pagewanted=1&_r=0

[758] Israel, Esteban, and Anthony Boadle, "Brazil to insist on local Internet data storage after U.S. spying", *Reuters,* 28 Oct 2013.
http://www.reuters.com/article/2013/10/28/net-us-brazil-internet-idUSBRE99R10Q20131028

[759] Smith, Chris, "Twitter adds another layer of security to keep out the government snoops", *Tech Radar*, 23 Nov 2013. http://www.techradar.com/news/internet/twitter-adds-another-layer-of-security-to-keep-out-the-government-snoops-1202147

United States has played in the country's post-war history.[760] A couple of months later, when she discovered her mobile calls were being intercepted, she was not quite so relaxed about it.

While the media attention has been on the extent of the NSA's surveillance, it has not focussed so much on the extent of surveillance by companies such as Google, Facebook, Amazon, Yahoo and other large multinationals. However, if a whistle blower were to leak how extensive surveillance by these companies has been, there might be similar outrage.

Conclusions relevant to the IRISS project

Failure of oversight

Stephen Walt, Harvard professor of international affairs, states, "Once a secret surveillance system exists, it is only a matter of time before someone abuses it for selfish ends."[761] Hence, there is an apparent need for oversight of such systems. However, as the NSA revelations have continued, it has become obvious that the intelligence agencies in the US and UK (and perhaps elsewhere) have lacked proper oversight. *The New York Times* commented that "Despite the agency's embrace of corporate jargon on goal-setting and evaluation, it operates without public oversight in an arena in which achievements are hard to measure."[762] In late October 2013, Congressional Democrats and Republicans introduced a bill that would curb some of the NSA's practices. Representative John Conyers Jr., Democrat of Michigan, a sponsor of the bill, said at the time that "Our intelligence community has operated without proper congressional oversight or regard for Americans' privacy and civil liberties."[763] The issue of oversight of the intelligence agencies is now firmly on the public agenda.

In the UK, at the first public hearing of the parliamentary Intelligence and Security Committee (ISC), GCHQ director Iain Lobban, head of MI5 Andrew Parker, and head of MI6 John Sawers all said the current oversight system is working well and there was no pressing need to update technology-neutral laws as the principles of necessity and proportionality within the law were sufficient to guide the actions of the intelligence agencies.

---

[760] Eddy, Melissa, "Merkel Appears to Weather Anger among German Voters over N.S.A. Spying", *The New York Times*, 11 July 2013. http://www.nytimes.com/2013/07/12/world/europe/merkel-seems-to-weather-german-anger-over-nsa-spying.html?_r=0

[761] Walt, Stephen, "Snowden deserves an immediate presidential pardon", *The Financial Times*, 8 July 2013.
http://www.ft.com/cms/s/0/0ccf2d14-e7c1-11e2-babb-00144feabdc0.html#axzz2YiI70RAU

[762] Shane, Scott, "No Morsel Too Minuscule for All-Consuming N.S.A.", *The New York Times*, 2 Nov 2013.
http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?src=un&feedurl=http%3A%2F%2Fjson8.nytimes.com%2Fpages%2Fworld%2Feurope%2Findex.jsonp

[763] Landler, Mark, and Michael S. Schmidt, "Spying Known at Top Levels, Officials Say", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/officials-say-white-house-knew-of-spying.html

Not everyone shares their views. If anything, the NSA revelations have made abundantly clear, the failure of oversight. Gus Hosein, executive director at Privacy International, told the LIBE committee of the European Parliament that the UK parliamentary committees, supposed to keep intelligence services in check, have become nothing more than "cheerleaders" for those intelligence agencies. He said there had been no discussion of the NSA's PRISM surveillance programme or GCHQ's TEMPORA fibre-optic tapping programmes by the UK Parliament's Intelligence and Security Committee prior to Snowden's whistleblowing.[764]

The Financial Times and *The Guardian* both found the UK's Intelligence and Security Committee (ISC) wanting; the members failed to provide the spymasters with a tough grilling.[765] Sources subsequently told *The Sunday Times* that the heads of MI5, MI6 and GCHQ agreed to appear before the ISC on the condition that they were told the questions beforehand – which led one MP to comment: "'Evidently the whole thing was a total pantomime."[766]

A Conservative MP in the UK has suggested parliamentary oversight of surveillance could be improved if the ISC were chaired by a member of the opposition to ensure its independence and be freely elected by MPs.[767] Transparency – in making such hearings public, as occurred when the spymasters appeared before the ISC – should also help improve oversight, but on this occasion, the transparency was a charade. Not providing or agreeing questions beforehand with those appearing before the committee would have been a wiser course of action. Subjecting the spymasters to interrogation by the media might have led to tougher questions. Even so, the spymasters felt sufficiently powerful that they could, and did, refuse to answer questions on the grounds of national security. However, if spymasters refuse to answer such questions, at least in camera, then it becomes another indication of the breakdown of democracy.

The bane of the privacy–security trade-off paradigm

The NSA revelations have shown how endemic and widespread nature of the paradigm of a "balance" or "trade-off" between security and privacy. For example, when the Spanish government summoned the American ambassador to address allegation that the NSA had been surveilling the Spanish population, the ambassador told reporters afterwards that "Ultimately, the United States needs to balance the important role that these programs play in protecting our national security and

[764] Ashford, Warwick, "NSA and GCHQ mass surveillance violates EU law, study finds", *ComputerWeekly.com*, 8 Nov 2013. http://www.computerweekly.com/news/2240208711/NSA-and-GCHQ-mass-surveillance-violates-EU-law-study-finds

[765] Blitz, James, "Parliamentary panel fails to serve up a good grilling", *The Financial Times*, 7 Nov 2013.
http://www.ft.com/cms/s/0/fb09950a-47d9-11e3-b1c4-00144feabdc0.html#axzz2jztTy1by; Weaver, Matthew, "Key questions the chief spooks were asked, and those they did not hear", *The Guardian*, 8 Nov 2013.
http://www.theguardian.com/world/2013/nov/08/nsa-leaks-parliamentary-questions-analysis

[766] *Daily Mail*, "So much for the interrogation: Spy chiefs knew what questions were going to be asked BEFORE parliamentary committee", 17 Nov 2017.
http://www.dailymail.co.uk/news/article-2508779/Spy-chiefs-fed-questions-advance-parliamentary-committee-hearing.html

[767] Quinn, Ben, "Tory MP adds to calls for improved oversight of UK intelligence services", *The Guardian*, 5 Nov 2013. http://www.theguardian.com/world/2013/nov/05/tory-mp-intelligence-services

protecting the security of our allies with legitimate privacy concerns." Ironically, Spanish secretary of state Iñigo Méndez de Vigo, in a separate statement, referred to the same paradigm when he said there was a need to maintain "a necessary balance" between security and privacy.[768]

The Obama White House uses this paradigm, as when a spokesman said: "The president welcomes a discussion of the trade-offs between security and civil liberties." Use of this paradigm has appeared in public opinion surveys. The Angus Reid Global survey, found public support for the argument that security and anti-terrorism efforts include trade-offs against civil liberties and personal information privacy.[769] In the survey of Canada, the US and the UK, the pollsters found that 60 per cent of UK respondents took this view, compared with 54% of Americans. Canadian public opinion was almost evenly split on the issue (49% vs 51%).[770]

The media also use the balance metaphor.[771] In spite of the fact that various officials, politicians, the media and others refer to the need for a proper balance between privacy and security, the metaphor is a red herring, conceptually flawed and downright dangerous for civil liberties. If privacy is traded off against national security, individual privacy will always lose out to collective security, even though privacy is a cornerstone of democracy. Many experts and academics have discredited the trade-off paradigm.[772] It is possible to have both privacy and security, without reducing one or the other. A better paradigm is risk management, i.e., to identify risks to privacy and security, either separately or together, and, preferably in consultation with stakeholders, to identify ways of overcoming those risks with no or minimal negative impacts on privacy and/or security.

Although senior industry people seem to think in terms of the trade-off paradigm, Google Executive Chairman Eric Schmidt said the right balance of security and privacy starts with finding the appropriate level of oversight. "There clearly are cases where evil people exist, but you don't have to violate the privacy of every single citizen of America to find them."[773] The balance paradigm may be wrong, but the oversight is surely right. Ironically, many regulators struggle to provide adequate

---

[768] Minder, Raphael, "Spain Summons American Ambassador on New Reports of N.S.A. Spying", *The New York Times*, 28 Oct 2013.
http://www.nytimes.com/2013/10/29/world/europe/spain-calls-in-us-ambassador-in-spying-scandal.html?_r=0

[769] Angus Reid Global, "More Canadians & Britons view Edward Snowden as 'hero' than 'traitor', Americans split", 30 Oct 2013. http://www.angusreidglobal.com/polls/48837/more-canadians-britons-view-edward-snowden-as-hero-than-traitor-americans-split/

[770] Ibid.

[771] "The disclosures of the National Security Agency's activities by a former contractor for it, Edward J. Snowden, have set off a fierce debate on both sides of the Atlantic about the proper balance between privacy and economic, security and other interests." Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013.
http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html

[772] See, for example, Zedner, Lucia, *Security*, Routledge, Abingdon, [UK], 2009, pp. 134-137.

[773] Kan, Deborah, "Google Chairman Lambastes NSA Actions as 'Outrageous'", *The Wall Street Journal*, 4 Nov 2013.
http://online.wsj.com/news/articles/SB10001424052702304391204579177104151435042

oversight of Google itself. The surveillance in which Google is engaged is arguably just as damaging to privacy as that of the NSA.

Jo Glanville, the chief executive officer of English PEN, has said that keeping the country safe does not entitle the government or the intelligence services to act without regard to our human rights. Glanville, importantly and correctly, made the point that "They are not mutually exclusive. It is possible to conduct targeted surveillance with effective oversight while according respect to all our rights."[774]

Unanswered questions

The Snowden revelations have raised a host of issues for Europe as well as other countries. Among these issues are the following:

To what extent are European countries able to protect their citizens from unauthorised surveillance by the US?

To what extent is the US threatening European economic interests by US surveillance of European trade negotiations and strategy?

Is the US gaining an unfair advantage over European companies by its surveillance?

Is European press freedom threatened by comments from David Cameron to stop *The Guardian* and other newspapers from continuing to publish leaked information?

Are political leaders simply embarrassed by the revelations and, to cover their embarrassment, make comments that the revelations are damaging national security?

Are intelligence agencies sufficiently accountable to elected representatives?

Should secret laws be permitted in an open democracy?

Could the NSA influence the outcome of elections in Europe (or elsewhere) by leaking damaging information about a candidate?[775]

What do we have to fear as ordinary citizens? As we know, there is the problem of information overload: the needle in the haystack will not be found easily and the less so, the bigger the haystack. With regard to personal data and privacy, we do not know what algorithms are applied to the data scooped up by the NSA, and whether we will be swept up as part of the dragnet. Certainly, that is the rational basis of public concerns about the extensive NSA surveillance. But what are the chances of that happening for otherwise ordinary citizens? We don't know. Nor do we know how

[774] Quinn, Ben, "Tory MP adds to calls for improved oversight of UK intelligence services", *The Guardian*, 5 Nov 2013. http://www.theguardian.com/world/2013/nov/05/tory-mp-intelligence-services

[775] A recent example of an attempt by an intelligence agency to influence a democratic election is recounted here: Sang-Hun, Choe, "Prosecutors Detail Attempt to Sway South Korean Election", *The New York Times*, 21 Nov 2013. http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html?_r=0. "Prosecutors have indicted several top intelligence officials, including Won Sei-hoon, the former director of the spy agency [the National Intelligence Service of South Korea], on charges of ordering an online smear campaign against opposition candidates in violation of election law."

metadata are analysed, and what it takes to end up on the screens of the secret services.

The main drivers for the whole surveillance process are heavily economic in nature: industry wants to sell their equipment and services, and big corporations want to protect their (online) assets from espionage. This economic rationale is reinforced by administrative logic and political strategies, i.e., the intelligence agencies want to increase their powers and the political actors want to make sure they have taken any necessary precautions to protect their homelands from terrorists.

The breakdown of open democracy

If the leaked documents were a revelation to the American and European peoples, they were also a revelation for some of their political leaders. According to the Liberal Democrat former cabinet minister Chris Huhne, neither the cabinet nor the National Security Council was informed about the PRISM and TEMPORA programs. "The cabinet was told nothing about…their extraordinary capability to vacuum up and store personal emails, voice contact, social networking activity and even internet searches," he wrote in *The Guardian*.[776] Similarly, reports suggest that Obama did not know that the NSA was intercepting Angela Merkel's mobile phone.[777]

The Snowden revelations have led to a breakdown in trust, as various European leaders have said, between Europe and the US. Trust is easy to break, but hard to repair. But the issue of trust is not only between Merkel and Obama, and other political leaders, but also between citizens and their leaders. In the UK, citizens have to trust a government committee whose members are themselves not trusted to know about the most significant surveillance programs.[778]
The New York Times has commented that "To casually permit this surveillance — with the American public having no idea that the executive branch is now exercising this power — fundamentally shifts power between the individual and the state, and it repudiates constitutional principles governing search, seizure and privacy."[779]

The NSA revelations call into question the nature of our democracies. It puts a whole new spin on the open nature of democracy, i.e., the openness of our democracy has made it easy for the NSA to exploit. The safeguards against abuse have been inadequate. Can a government of the people for the people exist when powerful minorities completely overwhelm democratic values? According to Guardian editor Alan Rusbridger:

> The security apparatus is today able in many democracies to exert a measure of power over the other limbs of the state that approaches autonomy: procuring legislation which prioritises its own interests over individual rights, dominating

[776] Rusbridger, Alan, "The Snowden Leaks and the Public", *The New York Review of Books*, Issue of 21 Nov 2013. http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/?pagination=false
[777] *The Economist*, "Cloaks off", 2 Nov 2013. http://www.economist.com/news/international/21588890-foreign-alarm-about-american-spying-mounting-sound-and-fury-do-not-always-match-0
[778] Rusbridger, op. cit. 2013.
[779] The Editorial Board, "President Obama's Dragnet", Editorial, *The New York Times*, 6 June 2013. http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html?pagewanted=all&_r=

> executive decision-making, locking its antagonists out of judicial processes and operating almost free of public scrutiny.[780]

The Observer, the sister newspaper to the Guardian has seen the dangers to democracy. The newspaper carried an item in which the following comment was made:

> The "mess" that the NSA (and our own dear GCHQ) has landed us in is a symptom of a major failure of our political systems. All democracies are impaled on the horns of the same dilemma: they need openness, because the consent of the governed requires that people know what is being done in their name; but sometimes openness undermines the efficacy of the secret (and perhaps necessary) things that are done in their name. The choice is then between sacrificing accountability or sacrificing secrecy… We urgently need something better and if we don't get it then we could be, as one spook put it, "a keystroke away from totalitarianism".[781]

A Conservative backbench MP, David Davis, has expressed strong support for the role played by Snowden and argued that "The only protection for us all in this sort of area is actually whistleblowers. It's the only thing that makes these sorts of organisations behave properly."[782]

It seems appropriate to conclude this section with a statement from Edward Snowden, one that he made (in writing) to the European Parliament's LIBE committee:

> The surveillance of whole populations, rather than individuals, threatens to be the greatest human rights challenge of our time…. A culture of secrecy has denied our societies the opportunity to determine the appropriate balance between the human right of privacy and the governmental interest in investigation. These are not decisions that should be made for a people, but only by the people after full, informed, and fearless debate. Yet public debate is not possible without public knowledge, and in my country, the cost for one in my position of returning public knowledge to public hands has been persecution and exile. If we are to enjoy such debates in the future, we cannot rely upon individual sacrifice. We must create better channels for people of conscience to inform not only trusted agents of government, but independent representatives of the public outside of government.[783]

Resilience in a surveillance society

The Snowden revelations have not been a uniform horror for privacy. While the extent of surveillance in society is far greater than most people might have managed, the revelations have served to demonstrate resilience and resistance too.

If one were to ask how resilience can be operationalised, one could consider at least two different paradigms. Nominally, one paradigm for resilience in a surveillance society might be like that of a command centre that takes various measures to

---

[780] Rusbridger, op. cit. 2013.
[781] Naughton, John, "Why the NSA has landed us all in another nice mess", *The Observer*, 1 Dec 2013.http://www.theguardian.com/world/2013/dec/01/nsa-edward-snowden-survelliance-internet
[782] Quinn, Ben, "Tory MP adds to calls for improved oversight of UK intelligence services", *The Guardian*, 5 Nov 2013. http://www.theguardian.com/world/2013/nov/05/tory-mp-intelligence-services
[783] Snowden, Edward, Statement to the LIBE Inquiry meeting of 30 September 2013. http://www.europarl.europa.eu/committees/en/libe/events.html?id=hearings

stimulate societal resilience and/or resistance to the increasing prevalence and pervasiveness of surveillance in society. Another paradigm might be that resilience is like a mesh network: it builds across society, with no central point. In other words resilience becomes viral and out of the hands of any central authority.

The Snowden revelations, however, present an interesting exercise in mapping resilience amongst different stakeholders in a surveillance society. In this case, one person, Edward Snowden, a whistle-blower of heroic proportions (in more senses than one) leaked thousands of documents showing the NSA engaging in mass and targeted surveillance. He leaked the documents to two journalists, Glenn Greenwald and Laura Poitras, and those journalists broke the story in *The Guardian* which then created a media sensation as other newspapers, especially including *The New York Times* and *The Washington Post*, picked up the story and started to publish some exclusives based on leaked documents. While *The Guardian* has continued to publish exclusives, many other newspapers and media outlets in various other countries – Germany, Spain, the Netherlands, Australia, Brazil, Indonesia, etc., have been publishing "exclusives" too. Snowden claims not to have kept any documents on his laptops or memory sticks when he flew from Hong Kong to exile in Moscow. Thus, the media have been passing leaked documents among themselves. So in terms of news flow, we see a phenomenon of one (Snowden) to two (Greenwald and Poitras) to many.

In terms of the societal response to these stories, there have been many. The public in general and many politicians (those spied upon especially) have expressed outrage. Their awareness of surveillance has certainly been ratcheted up a lot. While people may be "coping" with a new awareness of how extensive surveillance is, there has been a lot of resistance too.

In efforts to counter mass and targeted surveillance, many people, political leaders, industries and other stakeholders are taking a range of political and technological measures to increase their privacy. Some of these efforts are co-ordinated, many are not.

Citizens are adopting technologies and services to protect their privacy. So are companies such as Google, Yahoo, Twitter and others, by encrypting links between their servers. It is difficult to say how successful these efforts will be in countering the depredations of the intelligence agencies, but at least efforts are being made. Other businesses are protesting surveillance and secret orders to reveal who are using their services: Lavabit has taken the extraordinary measure of shutting down its business altogether.

Brazil, Germany and other countries are considering efforts to keep traffic within their countries or at least forcing foreign-based businesses wanting to provide services in their countries to meet their standards and requirements. Brazil and Germany have also co-sponsored a resolution at the UN to roll back surveillance.

The European Parliament has reinstated Article 41 (1) in the proposed Data Protection Regulation. MEPs and data protection authorities are renewing their scrutiny of the Safe Harbor agreement. The European Parliament (the LIBE committee) has been holding expert hearings.

The public are expressing their views in many uncoordinated ways – e.g., in their comments to news stories, in their petition to the White House to pardon Snowden, in placing adverts on buses in Washington about Snowden and so on.

The public is also expressing its lack of trust in politicians and other institutions in opinion polls. Obama, especially, will have to do a lot to re-establish trust in his government.

There is a ground swell of public opinion questioning how extensive surveillance needs to be. The issue is now high on the public agenda and politicians will need to develop a policy on what is acceptable, and try to convince voters that they can be trusted to take public opinion into account. One can expect better oversight of the intelligence agencies in the weeks, months and perhaps years to come.

In resilience terms, people and organisations are both "coping" and taking anticipatory measures. They assume that this high level of surveillance will continue, hence they are "anticipatory" – they are taking technical measures (e.g., to encrypt communications) to protect their communications as well as social measures (such as those mentioned above) that anticipate continued surveillance but also, at the same time, are acts of resistance.

Thus, as a paradigm of resilience in a surveillance society, we have witnessed a mixture of both resilience (as coping and as anticipatory) and resistance, in short a blending of the two above-mentioned paradigms. Above all, the Snowden revelations show us that resilience builds from communications, whether one-to-many or many-to-many.

The next section outlines a set of recommendations that can further strengthen resilience and resistance to the extent of surveillance in society today.

Protecting privacy in a surveillance society – a way forward

The default setting in political, corporate and societal thinking is that there should be no mass surveillance unless any particular system can be justified, starting with a privacy impact assessment, review by a regulatory authority and parliamentary oversight committee.

Governments and companies should be obliged, thereby, to undertake privacy impact assessments, which should include stakeholder engagement, publication of the PIA report and independent, third-party review.

Existing mass surveillance systems that have not been subject to a privacy impact assessment should be reviewed and terminated where there is no good justification for such systems.

Parliamentary or congressional oversight committees should be, as recommended above, led by a member of the opposition.

Transparency is essential if governments (and corporate leaders) are to rebuild trust. There should be no secret laws.

Politicians, such as Angela Merkel, are right to feel aggrieved about the extent to which they have been subject to surveillance by the NSA or other intelligence agencies. But the public is entitled equally to feel aggrieved. While politicians of allies should not be subject to surveillance, neither should the public.

Mass surveillance operations that endanger the privacy of citizens should be terminated. While terrorism is intolerable, the rape of privacy in a democracy is also intolerable. Intelligence agencies need to find more targeted alternatives for apprehending terrorists.

To protect privacy in a surveillance society, society needs to impose controls on surveillance, specifically, political leaders and regulators must introduce legislation that places controls on, especially, mass surveillance systems, whether they are governmental systems or private systems created by Google, Facebook, Amazon etc.

Governments, especially, should conduct regular opinion surveys to have an unbiased understanding of what the public thinks of surveillance (and its extent) in society.

Parliaments should have independent annual reports on the state of privacy and surveillance, which should include recommendations on how citizens, groups and society can better protect privacy.

In the final analysis

What we have presented so far is the emergence of a debate over the legitimacy of surveillance in contemporary societies, triggered by the revelation of a single individual and distributed through media channels.

Looking at the recent events and discussions in the wake of the Snowden revelations from a perspective of social and political theory, a number of issues emerge that point beyond the immediate debate over the questionable practices of the intelligence-industrial complex. The events can be placed in a larger context of social and cultural patterns of social integration, governance and control. Taking this wider perspective can help better understand how to adequately react to the problems identified by an individual whistle-blower and the subsequent investigations by media and surveillance activists.

One of the important questions raised by this affair is whether a society as a whole in the medium of public discourse can develop a balanced and reasonable understanding of the threats and dangers and how these should be addressed.

From ancient times, cultures have developed ideas about their powerful enemies. The inner social working of groups was threatened by the wrath of gods, by external demons, by hostile neighbours, brute force of nature, pandemics or other forces of evil. What all these evil forces had in common was their intangibility. Present day societies display a similar ecology of fear. They develop popular images of imminent threats to social order, life and limb of the citizens. A whole pandemonium of threats can be brought into the foreground to justify an array of remedial actions. From a sociological perspective, these threats work as mechanisms to mark and maintain the

boundary of a social group or society. They introduce the distinction between "Us" and "Them". In the age of globalised, multi-cultural, multi-ethnic, trans-national, media-driven societies, it becomes difficult to sustain such boundary maintenance mechanisms. While in the recent past, during the so-called bipolar world order, such a boundary could be drawn by pointing to communism as the dominant threat to the "Free West", today we see a shift from the East-West to the North-South divide. The dominant threat is construed no longer along ideological lines but along religious and cultural lines. Jihadists and Islamic fundamentalists, operating from the global South, have replaced communist agitators and infiltrators.

Taking this analytical perspective, a number of politically salient topics can be interpreted as means to maintain the boundary of the social group at different scales. Public concern about climate change, global warming and pollution re-creates "Nature" as the "Other" to society. Threats emanating from beyond the social sphere jeopardise the very survival of mankind. Beyond these global threats, suitable 'enemies' defining the line between Us and Them: criminals, welfare mothers, drug addicts and many others can be activated as popular images to demonstrate who the good guys are and where the realm of evil begins against which law-abiding citizens have to be protected.

These threats have a number of features in common: they are made visible and tangible by the media; they require massive surveillance to be kept under control and some sort of remedial action curtailing the freedom of citizens seems necessary to combat these threats. Take the ozone hole as an example: as a hybrid object comprised of scientific observation, political discourse and massive media coverage, it emerges in society carrying with it the warning to change consumption and production patterns of industrial economies. The threat comes from outside, threatens society and requires urgent action. The same could be said about criminals, drug users, Jihadists and Islamic fundamentalists. They emerge as objects of public concern and policy, coming from outside the realm of our life world, threatening social order and made visible as objects of fear primarily through media coverage. To understand the logic of this ecology of fear, fuelled by different types of public enemies, one has to understand the dynamics and working of public media discourse. The media compete for a share of voice, and public attention is limited. Public policy is tied into this process of generating arousal and concern, rallying for support for remedial action. In order to establish an object or group as an imminent and massive threat to society many different actors and stakeholders have to cooperate: media, policy actors, social movements, and other groups and organisations have to pool their resources in order to create the momentum for a successful campaign establishing a sustainable idea of an enemy in the public consciousness.

What makes the Snowden revelations stand out in this game of media-amplified construction of public enemies is the reversal of the logic. Instead of focussing on the threats posed by an external enemy, the remedial actions to combat the presumed threat were scandalised. This has created the rare situation of a balance of means among proponents and critics of the political game of fear. What Snowden and all the others publishing the information he collected did, was to turn the logic of the media against a security-political-industrial complex distributing images of an imminent threat using the very same mechanisms. Applying the notion of boundary maintenance, this, perhaps for the first time created a situation where a substantial

portion of the general public started to entertain the idea that the cure might be worse than the disease. Instead of strengthening social cohesion by focussing on the external enemy, people questioned whether they could rely on some of their entrenched beliefs about the working of the state. This seemed to trigger a hitherto unknown activity of what could be called practices of self-defence against actions of state authorities targeting the private sphere of the citizens.

While at first glance the massive surveillance of citizens can be seen as a serious attack on public discourse and democratic procedures, the controversial debate about these practices has also fuelled a new debate about adequate protection against an intrusive state, spying indiscriminately on its population. Probably with hindsight the Snowden revelations will appear historically as one of the single most important irritants of the general public's trust in the legitimate exercise of state power. By the same token, the public may start to question the threat assessments flagged on a regular basis by the security-industrial-political complex. How threatening are the threats? How successful are the means to counter them? This type of questioning, hitherto entertained primarily among a small group of experts and critics of present-day surveillance practices, is now entering the front pages and talk shows. National intelligence services in several European countries have come under pressure to defend their practices and present proof of successful actions in combatting crime and terrorism.

At the same time, public attention has turned to a couple of other problems regarding the idea of privacy, democratic self-governance and rule of law. As the events have clearly demonstrated, legal safeguards as such are not a guarantee against mass surveillance. The intelligence community was acting legally (at least, to some extent), albeit the legal regulations were problematic from a political and democratic perspective. Laws were tailored to the demands of the intelligence community or had a built-in backdoor that permitted the expansion of surveillance under the pretext of security threats. However, these threats are difficult to substantiate.

One of the main argumentative frames applied in the controversy about the limits of surveillance draws on the metaphor of balancing freedom (or liberty or privacy) and security. Citizens are asked to trade some of their freedoms in exchange for increased security. More surveillance is supposed to produce a more secure society and the intrusion upon their privacy is what the citizens have to trade in for this. A closer look at this metaphor reveals its shortcomings. The balancing model operates with three actors or groups: the general public or the citizens, the state or the intelligence and law enforcement agencies and a third group that could be termed the target group, e.g., the undetected perpetrators who are supposed to be hindered from causing future damage. The target group, according to this logic, hides somewhere among the members of the general public and hence the public has to be targeted by mass surveillance to identify the members of the target group. The measures are justified by damage caused to society caused by attacks from the target group. A simple thought experiment helps to demonstrate the built-in biases of this approach. If we replace the target group of terrorists with the target group of financial institutions (while leaving the overall logic of the argument as it is), the bias becomes obvious. We can easily demonstrate that not all individuals working for the financial sector follow a criminal path. Nonetheless, being a member of this sub-culture entails the risk of becoming radicalised and engaging in illicit behaviour (e.g. selling securities to clients and

simultaneously placing bets against them). This can cause massive damage and so it would be perfectly rational, following the reasoning of the balancing metaphor, to trade in some of the freedoms enjoyed by the financial institutions for greater security for society as a whole. Additionally, there are international networks involved in these illicit transactions, a hedge fund as an organisation can display a structure similar to a Jihadist group – entities or people spread across the globe cooperating and communicating among each other transferring funds without being exposed to full scrutiny of state institutions or working actively to prevent such scrutiny.

What the above hypothetical exercise demonstrates is the moral and political dimension of surveillance practices. Sacrificing civil liberties for a cause may be justified, depending on the cause and the domain. While the basic idea of imposing controls and curtailing certain freedoms for certain groups in a liberal society may be justified, the mass surveillance of whole populations is not acceptable. This line of reasoning raises issues of a moral economy and reflexively points to a process of democratic deliberation, addressing the question: what should we as a society do to prevent substantial damage to the polity? What do we conceive as such damage and finally, what are we willing to trade in to protect us from future damage?

Taking the perceived threat of a terrorist attack out of the narrow frame of a group of determined criminals targeting "our" societies, can create a broader and more comprehensive understanding of the underlying problems. It can also foster a more complex understanding of the different trade-offs and balances involved in the debate about security. Introducing a third element into the equation of security versus liberty and/or privacy demonstrates this quite clearly. This third element could be called "convenience". The use of electronic communication media makes many activities of daily life more convenient or "user-friendly", while at the same time producing the data on which the intelligence community relies: mobile phones, social media, online shopping, credit cards, Internet browsing create the infamous 'data doubles' of citizens that can be monitored by the intelligence services to identify suspicious behaviour, find evidence for future deviance or detect potential perpetrators.

Establishing a more responsible use of this convenient infrastructure would entail a change in established modes of action – from encryption to changes in consumption patterns. But convenience in this context can also be spelled out in a different way. The life style of modern consumer society rests on a severe imbalance at the global level between the rich North and the impoverished south. This imbalance creates an unequal distribution of resources and produces economic, social, cultural and ecological problems of a global scale. Increasing wealth in northern countries creates poverty in the global south and poverty breeds radicalisation. Awareness of the social and economic dynamic fuelling processes of political radicalisation seems to be growing in the wake of the debate about mass surveillance. The threat assessments produced to justify the surveillance of global communication streams, of migration and mobility focussing on those geographical areas from which the perceived threat of terrorist attacks is supposed to originate begs the question as to whether Western open democratic societies should pay the price of such highly intrusive mass surveillance and a politics of exclusion, creating, for example, a "Fortress Europe" to protect against an enemy who could turn out to be a rebel with a cause. Looking at the strategic objective of the terrorists, one could argue that they seem to have succeeded

in creating a deep paranoia simply by launching a few unpredictable attacks and perpetuating fear of new, future strikes.

In terms of resilience, we see a kind of collateral enlightenment and broadening of the public debate about surveillance, the state and some fundamental assumptions about contemporary societies. A society experiencing massive, uncontrolled and even illegal practices of surveillance enters into a sobering process of looking at itself and begins to question its own institutional and legal set-up against the fundamental values of democracy, accountability and openness.

3.4 HORIZONTAL ANALYSIS OF ADVERSE EVENTS

This section provides a horizontal (or comparative) analysis of the adverse events described in sections 3.2 and 3.3 above. The objective is to see whether adverse events have led to more surveillance in society, how they have impacted privacy and whether there are lessons about resilience to be learned their analysis.

3.4.1 Nature of the adverse event

The IRISS partners selected a variety of adverse events for analysis. We were particularly interested in adverse events that might have prompted some increased use of surveillance. Of the 11 adverse events discussed above, several were terrorist attacks, namely, those of 11 September 2001, the London, Madrid and Boston bombings, and the Mumbai attack. Several adverse events are characterised by some form of wrong-doing and rights violations, even if they were not terrorist attacks as such – the 2008 Global Financial Crisis, the Google Street View case, the UK National DNA database and the school shootings in Germany. Some events explicitly and directly involved surveillance, e.g. NSA revelations. Only one event was the result of a natural disaster (the Christchurch earthquake). Most of the selected adverse events occurred in Europe (the London and Madrid bombings, the school shootings, the UK National DNA database). The others occurred in widely disparate places outside Europe – the Christchurch earthquake (New Zealand), the 9/11 attack and Boston bombing (US), the Mumbai attack (India). Some were global events, e.g., the Street View collection of Wi-Fi data and the NSA revelations. The adverse events were not selected to be particularly representative of anything other than what they are – adverse events which involved or led to an increase in surveillance. The diversity of places where the adverse events occurred helps us see if there were any differences in national responses to such events. Almost all of the events took place in the last 10 years. The exception was the 9/11 attacks. The events also had a range of effects and impacts (some involved a large number of deaths, others had both deaths and injuries, yet others had other types of impacts such as financial hardship, loss of home and property, mental stress, loss of privacy, chilling effects – some of these impacts are measurable and others are hard to measure).

3.4.2 Institutional responses

As one might expect, institutional responses to the adverse events have varied.

In Spain, the adverse event led to political recriminations. In the three days between the bombings and the general election, the main political parties in Spain accused

each other of concealing or distorting evidence, and the governing party blamed ETA for the bombings. In the election, the Spanish Socialist Workers' Party under José Luis Rodríguez Zapatero replaced the conservative Partido Popular government of José María Aznar, who was the biggest political casualty of the event. A few weeks after the election, the new government withdrew Spanish troops from Iraq. Surveillance, especially on trains and in train stations, increased significantly in response to the bombings.

Subsequent reviews about how well the emergency services coped with the terrorist attacks in London also vary in their assessment, but in general, the response seems to have been quick and efficient. The emergency services followed a well-rehearsed drill ("Gold Command") set up for such a contingency and a practice exercise involving medics and the emergency services had been held not far from the location of the bombings just a few weeks earlier.[784]

In Mumbai, the simultaneous nature of the attacks created panic in the city and overwhelmed the security forces. The police control room systems were overloaded and personal devices were used for communication. Police units were deployed in "a haphazard and helter-skelter manner".[785] Some of the police, despite being only equipped for normal policing duties showed great bravery in dealing with the attackers.

The institutional response to the Street View collection of payload data in the UK at best can be said to be fractured, reactive and not at all geared to effectively address threats to society and its values based on frameworks that exist.

Following the school shootings in Germany, as with other adverse events, various politicians demanded intensified video surveillance at schools, new gun laws and better prevention. The most prominent demand was for a ban on violent computer games (so-called "killer" games), as politicians thought they were responsible for such events. Very few of these measures have been realised.

3.4.3 Judicial response/legal response

Perhaps the most notable legal response to the London bombings was the Terrorism Act 2006 which introduces various new offences relating to the preparation of terror attacks, such as training for a terrorist act, and to the "encouragement of terrorism", including criminalising the "glorifying" of terrorism. It also extends the period during which a terrorist suspect can be detained without charge to 28 days.

A Mumbai trial court sentenced Ajmal Kasab, the lone terrorist captured alive, to death on all 86 charges of his conviction. The Bombay High Court and the Supreme Court of India both rejected his appeals and upheld his death sentence.

In its judgment of 4 December 2008, the European Court of Human Rights (ECtHR) found that the blanket and indiscriminate nature of the powers of retention of the

[784] Segell, Glenn M., "Terrorism on London Public Transport", *Defense & Security Analysis*, Vol. 22, No. 1, 2006, pp. 45-59 [p. 47].
[785] Pradhan, Ram D., V. Balachandran, *Report of the High Level Enquiry Committee (HLEC) on 26/11,* 18 April 2009. http://maharashtratimes.indiatimes.com/photo.cms?msid=5289960

fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences failed to strike a fair balance between the competing public and private interests and, accordingly, the retention constituted a disproportionate interference with the applicants' right to respect for private life.

After the school shooting in 2009, the German gun law was amended, which meant new regulations on how and where private owners could and should store their weapons and guns. A registry of guns and gun owners is part of this process. The national registry has also helped to determine the number of privately held weapons in Germany.

3.4.4 Societal response

The immediate social response within Spain, and internationally, was to protest the attack and mourn its victims. Millions of people took to the streets in Madrid and elsewhere in Spain in massive demonstrations of collective grief. Many voters were outraged at the government's attempt to fix responsibility for the bombings on the ETA and gain political advantage against its Socialist opponents; this together with the government's unpopular support for the American-led intervention in Iraq, led to the defeat of the Parti Popular at the polls and the election of a new socialist government under Luis Zapatero.

The UK societal response to the "7/7" London bombings was varied and mixed. However, research on civil contingencies and disasters reveals that "the notion of mass panic has been largely discredited by the finding of orderly, meaningful mass behavior in disasters".[786] A telephone survey of 1,010 English-speaking adult Londoners was conducted a fortnight after the bombings to try to determine levels of stress and travel patterns among city residents. The survey found that 31% of respondents reported substantial levels of stress and while the majority displayed a certain resilience saying that "the bombings would have no impact on their travel plans", about a third said they would use public transport less and go into central London more rarely. In a follow-up study by the same research team seven months later, however, the 31% rate experiencing "substantial stress" "had fallen to 11%". Some critics have noted that "day-to-day harassment of Muslims through stop and search to high-profile police raids, has had a corrosive effect on the relations between Muslim communities and the police."[787] Greer has strongly challenged this thesis, arguing that "[t]here is no evidence to support it, and a great deal that points in the opposite direction".[788]

In upholding the death sentence of the Mumbai terrorist Kasab, the Supreme Court complimented the "resilient spirit of Mumbai that, to all outward appearances, recovered from the blow very quickly and was back to business as usual in no

[786] Drury, op. cit., 2009.
[787] Rubin, G. James, Chris R. Brewin, Neil Greenberg, John Simpson and Simon Wessely, "Psychological and behavioural reactions to the bombings in London on 7 July 2005: cross sectional survey of a representative sample of Londoners", *British Medical Journal*, doi:10:1136/bmj.38583.728484.3A, pp. 1-7, p. 1; 6;
[788] Greer, Steven, "Anti-terrorist Law and the United Kingdom's 'Suspect Muslim Community: A Reply to Pantazis and Pemberton", *British Journal of Criminology*, Vol. 50, 2010, pp. 1171-1190[p. 1171].

time".[789] The actions of individuals took centre stage during and after the Mumbai attacks. Individuals, in different capacities (either as employees, members of the police or security forces or as citizens) helped to reduce or mitigate the effects of the Mumbai attacks. These actions were documented live during the attacks and have even become case studies for business and crisis management. Nevertheless, one key public reaction was anger and resentment at being left vulnerable and the institutional lack of ability to prepare for and defend against such attacks.

As shown before, civil society organisations in the UK (and elsewhere) censured Google's collection of payload data in the media. They criticised the ICO's response to the incident very sharply.[790] Civil society organisations such as Liberty, GeneWatch and the Open Rights Group (ORG) were also severely critical of the DNA collection and retention regime.

Immediately after each school shooting in Germany, victims' families were met with psychological help and financial aid to cope with the aftermath of the shock that survivors, friends and family had experienced. The responses with the most impact on prevention and understanding did not come from the state or policy-makers, but from civil society and academia. The strategy is to find ways to prevent this kind of violence and raise the general sensitivity and awareness among pupils, teachers and parents. Almost all strategies that have been initiated following the events of the last 10 years aim to foster a sense of community and care amongst individuals.

3.4.5 Economic response

Within two months of the 11 March 2004 train bombings, the tourist industry in Spain claimed it was in "excellent health". Given that tourism constitutes 12 per cent of Spain's gross domestic product, the importance of demonstrating such buoyancy is highly relevant to an assessment of post-event resilience. This economically motivated public-relations reassurance that Madrid had been restored to normality ostensibly testifies to the city's resilience.

The 26 November 2008 attacks in Mumbai specifically impacted two well-known international brands – the Taj and Oberoi. Both the Taj and the Oberoi Trident reopened after the attacks with minimal economic fallout due to various measures they adopted in response and also due to the preventative measures they had in place before the attacks.

It is difficult to assess (and thus compare) the economic response to the collection of payload data by Google Street View, or biometic data by the national DNA database.

3.4.6 Media response

Media responses to the Madrid bombings in March 2004 were characterised by the use of cell phones and the internet to mobilise previously established networks for a

[789] *Md. Ajmal Md. Amir Kasab v State of Maharashtra*, Supreme Court, 29 August 2012. http://indiankanoon.org/doc/78874723/

[790] Petrou, Andrea, "ICO sent unqualified staff to investigate Google", *TechEYE.net,* 10 Nov 2010. http://news.techeye.net/security/ico-sent-unqualified-staff-to-investigate-google

protest that quickly spread as critiques and demands they were making resonated with an important segment of public opinion".[791]

Senior staff from the emergency services and from London Underground gave press conferences and briefed journalists "at the QE2 Conference Centre adjacent to the Houses of Parliament"; TV news gave extended live coverage throughout the day; and "a support center for victims and relatives was set up at the Queen Mother Sports Centre", also nearby. Additionally, "[t]he casualty bureau, set up to help people locate family members and friends, took 104,000 calls within the first 24 hours". CCTV cameras did not appear to deter nor help police in real-time co-ordination against the attacks, and "CCTV had only the most marginal of roles in the identification of the four bombers".[792]

Phythian quotes John Gray as arguing that: "by instantaneously disseminating the same images of carnage and panic throughout the world, the media have globalised our perception of terror. Governments behave as if this media apparition were an actual entity, with the result that the policies that are adopted in order to resist terrorism are ineffective and sometimes disastrously counter-productive".[793]

An analysis of "British Social Attitudes data collected between June and November 2005" examined "the readiness to trade off civil liberties for enhanced security", and found that after the July bombings citizens' concerns increased "significantly", with greater "willingness to trade off civil liberties for security", and moreover that "these perceptions [did] not revert to pre-attack levels". This study found that "the post-attack shift in public support for security policies at the cost of civil liberties – such as freedom of speech, rights of suspects... – is sizable". Interestingly, "this shift only manifests itself a week after the attack", suggesting a possible role of the news media, television coverage or public debate. [794]

Disturbingly, a study of "racially motivated hate crimes" carried out in England "in the wake of the 7/7 terror attack that hit London in July 2005 and the 9/11 terror attack that hit the US in September 2001" found "significant increases in hate crimes against Asians and Arabs that occurred almost immediately in the wake of both terror attacks and which lasted for a prolonged period. Moreover, hate crimes against Asians and Arabs do not return back to their pre-attack levels, showing a permanent increase in the wake of the attacks". The authors "hypothesise that attitudinal changes from media coverage act as an underlying driver".[795]

---

[791] Flesher Fominaya, Cristina, "The Madrid bombings and popular protest: misinformation, counterinformation, mobilisation and elections after '11-M'", *Contemporary Social Science*, Vol. 6, No. 3, 2011, pp. 289-307 [p. 289].

[792] Fussey, Pete, "Observing Potentiality in the Global City: Surveillance and Counterterrorism in London", *International Criminal Justice Review*, Vol. 17, No. 3, 2007, pp. 171-192 [p. 182].

[793] Gray, John, "A Violent Episode in a Virtual World", *New Statesman*, 18 July 2005, p. 16; cited in Phythian, Mark, "Intelligence, policy-making and the 7 July 2005 London bombings", *Crime, Law and Social Change*, Vol. 44, 2005, pp. 361-385 [p. 371-372].

[794] Bozzoli, Carlos and Cathérine Müller, "Perceptions and attitudes following a terrorist shock: Evidence from the UK", *European Journal of Political Economy*, Vol. 27, 2011, S89-S106, S89-S90; S101; S103.

[795] Hanes, Emma, and Stephen Machin, "Hate Crime in the Wake of Terror Attacks: Evidence from 7/7 and 9/11", Research Paper, November 2012. http://www.sv.uio.no/econ/english/research/news-and-events/events/guest-lectures-seminars/Thursday-seminar/paper/hanes-machin-november-2012.pdf

In the case of the BBC, "within six hours [it had] received more than 1,000 photographs, 20 pieces of amateur video, 4,000 text messages, and 20,000 e-mails". Richard Sambrook, then director of the BBC's World Service and Global News division, wrote that on the morning of 7 July, "audiences had become involved in telling this story as they never had before", and that public contributions "became an integral part of how the BBC reported the day's events".[796]

The way that people consumed news was also different from previous decades, and "for many Londoners, especially those who were deskbound in their workplaces, the principal source of breaking news about the attacks was the Internet". Websites, such as *BBC News* and *The Guardian* enabled ordinary users to submit their (in many cases, compelling and dramatic) first-hand accounts of events that morning.

The public played a role in the media reportage in the wake of the Mumbai attack too. Some individuals witnessing the attacks used their mobile phones and other devices to record events and disseminate information (written and pictorial, some of which raised ethical questions) through social media such as Facebook and Twitter.[797] The media's response to the attacks was two-fold: to function as means of communication and dissemination, and to carry out institutional review and oversight. The mass media (national and international) highlighted the institutional failures[798] such as that of the police and security forces in dealing with the attacks.[799] However, the media distorted the value of its good work by engaging in some sensationalism and irresponsible coverage of the attacks.

While there was not saturated media attention to Google's Street View's surreptiously recording personal data from Wi-Fi sites, nevertheless the media did play an important role in covering what Google was doing, especially when citizens formed a human blockade in some villages or towns where the Google-equipped vehicles were spotted. The media projected Google's collection of payload data in the UK in a number of ways: cautionary, expressing outrage, chastising. The media not only reported, they sometimes took an activist role as in the case of the *Daily Mail*'s David Thomas.[800]

Regarding the collection and retention of DNA samples and fingerprints in the UK, the media investigated and disseminated information (and thus created greater public

---

[796] Sambrook, Richard, "Citizen Journalism and the BBC", *Nieman Reports*, Vol. 59, No. 4, Winter 2005, pp. 13-16.

[797] Stelter, Brian and Noam Cohen, "Citizen Journalists Provided Glimpses of Mumbai Attacks" *The New York Times,* 30 Nov 2008. Beaumont, C. "Mumbai attacks: Twitter and Flickr used to break news", *The Daily Telegraph*, 27 Nov. 2008. Dolnick, Sam, "Bloggers provide raw view of Mumbai attacks", *MSNBC*, 30 Nov 2008. http://www.msnbc.msn.com/id/27984057/ns/technology_and_science-tech_and_gadgets/

[798] Swami, Praveen, "Mumbai attacks: One year on", *BBC News,* 25 Nov 2009. http://news.bbc.co.uk/1/hi/world/south_asia/8373836.stm

[799] For instance, Swami, Praveen, "Desperate Need for National Police Tactics and Weapons School", *The Hindu*, 11 Dec 2008.

[800] Thomas, David, "Why I'm going into battle with Google to find out if it stole my family's secrets", *Daily Mail Online,* 13 June 2012. http://www.dailymail.co.uk/debate/article-2158992/Why-I-m-going-battle-Google-stole-family-s-secrets.html#ixzz2QgnYgND7

awareness) about new developments on this subject.[801] BBC News dedicated a "Q & A" page to the National DNA Database; it published various articles on the retention term of DNA samples, criminalisation of people, questioned the size and purpose of the database, presented case studies on the role of DNA and the database, and highlighted the need for a debate on the subject. Bloggers (professional and amateur) posted information and stimulated debate on the unlimited collection and retention of samples and creation of profiles on the national DNA database.[802] Twitter users posted entries on the ECtHR Marper decision,[803] the national DNA database (the posts include information about the database, calls for debate, concerns about the database, its Orwellian potential and support for it). After the Marper decision in 2008, *The Guardian* highlighted how the Association of Chief Police Officers (ACPO) had advised senior police officers to "ignore a landmark ruling by the European court of human rights and carry on adding the DNA profiles of tens of thousands of innocent people" to the NDNAD.[804] McCartney explored the possible implications of the rapid expansion of the England and Wales National DNA Database (NDNAD) and highlighted how new risks are created, including not only error, improper access and disclosure and function creep but also the potential creation of a "suspect society" with forensic DNA technology co-opted into mass surveillance and social control mechanisms.[805]

The school shootings in Germany (and elsewhere) have generated an "uncountable number of newspaper and magazine articles".

3.4.7 Conclusions from an IRISS perspective

The unprecedented scale of the Madrid bombing, as well as its non-ETA Islamist source, made it a decisive, qualitatively different and shocking event that should be taken as the watershed for assessing resilience. The Madrid bombings also galvanised Europe's response to terrorism. Bilateral intelligence sharing increased. The European Commission created a new post and appointed Dutch politician Gijs de Vries as its counter-terrorism coordinator. His main role was to try and improve information sharing and co-ordinate and harmonise counter-terrorist legislation and co-operation between Member States. However, he had no formal operational role and a small staff.

The London bombings were also shocking events. In the case of the London bombings, we can identify "resilience" as featuring in several different ways – for

[801] For example, see *The Guardian*, "DNA Database". http://www.guardian.co.uk/politics/dna-database
[802] DNABoss. http://thednaboss.wordpress.com/blog/. A blog run by life science specialists; Katz, Deanne, "National DNA Database Comes under Scrutiny", *FindLaw,* February 2013. http://blogs.findlaw.com/blotter/2013/02/national-dna-database-comes-under-scrutiny.html; Wagner, Adam, "DNA Database: another key human rights election issue", *UK Human Rights Blog,* 19 April 2010. http://ukhumanrightsblog.com/2010/04/19/dna-database-another-key-human-rights-election-issue/. Palmer, Jessica, "EU court to Britain: your national DNA database violates human rights", *Bioephemera,* 11 Dec 2008. http://scienceblogs.com/bioephemera/2008/12/11/eu-court-to-britain-your-natio/
[803] A list of such tweets is available at: https://twitter.com/search?q=s%20and%20marper&src=typd
[804] Travis, Alan, "Police told to ignore human rights ruling over DNA database", *The Guardian,* 7 Aug 2009. http://www.guardian.co.uk/politics/2009/aug/07/dna-database-police-advice
[805] McCartney, Carole I., "Forensic DNA Sampling and the England and Wales National DNA Database: A Sceptical Approach", *Critical Criminology,* Vol. 12, No. 2, 2004, pp. 157-178.

example, resilience to terrorist attack, resilience to increased surveillance and psychological resilience. Perhaps displaying planned resilience in the wake of the 9/11 attacks in the US, the UK launched its CONTEST counter-terrorism policy in 2003 as a way of co-ordinating the UK Government's various responses to terrorism.[806] The policy has been revised and expanded since, and "funding has increased from £6 million per year in 2006 to £140 million in 2008/9"[807]. The CONTEST policy has four elements – arguably recognisable as different aspects of "resilience" – the essence of which the government has defined as:

- Pursue: to stop terrorist attacks;
- Prevent: to stop people becoming terrorists or supporting violent extremism;
- Protect: to strengthen our protection against terrorist attacks, and
- Prepare: where an attack cannot be stopped, to mitigate its impact.

Resilience measures can often learn from prior events and aim to mitigate future adverse events. However, resilience measures do not always anticipate very well their sometimes negative and counter-productive consequences.

People who were caught up in the bombing attacks displayed resilience. There are numerous instances and videos of survivors helping the wounded and recording the scenes of mayhem. While there were instances of pandemonium (which is different from panic), for example, in Mumbai, it is interesting and useful to note inherent, self-organising resilience under adverse conditions. Similar instances of inherent, self-organising resilience are often encountered in the wake of natural disasters too – i.e., people don't sit around waiting for emergency services to tell them what to do. Even before the emergency services arrive, survivors follow their common sense, help rescue or assist the wounded.

Thus, while resilience can be improved through planning and exercises organised by central authorities, it can spring from wellsprings that some people don't even know they possess.

Resilience can also be strengthened by reviewing what happened during adverse events. For example, Indian authorities set up a high-level committee to "analyse how far the existing procedures, instruments and administrative culture are to be blamed for what are perceived as lapses".[808] The committee sought to identify systemic failures and to recommend steps to mitigate future attacks.[809] There were similar reports after the London bombings; these efforts help to discover any lessons to be learned from the experience.

Some think resilience can be improved by the installation of more surveillance devices and granting police and counter-terrorism authorities' wider access to surveillance systems. For example, the aforementioned Mumbai Committee suggested

---

[806] House of Commons Home Affairs Committee, *Project CONTEST: The UK Government's Counter Terrorism Strategy*, Report HC 212, The Stationery Office Limited, London, 7 July 2009, p. 3.
[807] Briggs, Rachel, "Community engagement for counterterrorism: lessons from the United Kingdom", *International Affairs*, Vol. 86, No. 4, 2010, pp. 971-981 [p. 971].
[808] Appointed by the Maharashtra Government vide GAD GR No: Raasua.2008/C.R.34/29-A, 30 Dec. 2008.
[809] Pradhan, Ram D., V. Balachandran, *Report of the High Level Enquiry Committee (HLEC) on 26/11,* 18 April 2009. http://maharashtratimes.indiatimes.com/photo.cms?msid=5289960

the police be permitted access to CCTV cameras installed in private premises such as hotels, train private sector security personnel in handling such devices, underlined a need for a closer liaison between the Mumbai city police and mobile service providers to detect terrorist links, and recommended upgrading the Mumbai police's cellular monitoring capabilities.

New legislation is a typical outcome of attacks, presumably, in part because governments think that some new initiatives will improve resilience in case there are future adverse events and in part because governments want to be seen "doing something". This is exemplified by the US (the PATRIOT Act), the UK (Terrorism Act 2006), EU (the Data Retention Directive) and Mumbai (the National Investigation Agency Act 2008). The latter laid the foundation for the establishment of the National Investigation Agency (NIA), now India's central counter terrorism law enforcement agency.

The obvious risk with additional surveillance and new legislation is that the pendulum will swing too far towards improved security and, in the process, create new risks to privacy and other fundamental human rights. These new initiatives often involve more collection and exchange of personal data from other organisations, including those in third countries.

Surveillance infringements of privacy can create backlashes. For example, the Google Street View payload data collection incident arguably created and reinforced a broader general public awareness of privacy and data protection and a more specific sense of awareness of the dangers of exposing personal and sensitive personal data over (unsecured) Wi-Fi networks. To some extent, we could say that this prompted an increase in the use of encryption to protect privacy and personal data and a reduction in or more cautionary use of public unsecured Wi-Fi networks. This experience teaches us several things key amongst which are need for a more proactive and efficient approach to regulate privatised surveillance and its effects, culture of vigilance to surveillance, better co-ordination, sharing of information and learning of lessons between relevant authorities across the EU, and greater accountability, particularly on the part of industrial actors.

We also witnessed a threat in the unlimited collection and retention of DNA samples to a democratic society and its principles and values such as privacy, data protection, right to equal treatment, individual liberty in addition to ethical concerns. When exposed to this threat, society generally resisted. The positive elements evident in this case are:

- Ability of society to organise quickly (galvanise to action)
- Ability to disseminate information and raise awareness (on an ongoing basis)
- Addressing threats across domains (including cross-domain collaborations)
- Positive social context (establishment and wide acceptance of privacy and data protection rights)
- Ability of civil society to lead, influence society and decision-makers
- Capacity of individuals to take action
- Availability of suitable redress forums.

The conclusions drawn from a school shooting and a terrorist attack are somewhat different. While an event such as a school shooting may have horrific consequences, it

may not affect society as a whole in the same way as compared to the other analysed events. As with most of these events, the time span in which an event makes the headlines and is intensively discussed is typically rather short. The same holds true for the attention of politicians; they soon move on with other items on their agenda. This is not always true, however. There are exceptions: the NSA revelations coming from Edward Snowden were drip-fed to and by the media, so the "revelations" remained on the front pages for two months or more.

As with all classification systems, anything that classifies perpetrators or indicators of such events about to happen is in danger of producing false positives. Surprisingly, little attention has been paid to the implementation of technical devices such as video surveillance, metal detectors or human security, i.e., security personnel, in schools. All discussion involving such demands were met with great suspicion in Germany and died down very quickly.

Prevention in the case of terrorist attacks is largely a responsibility of intelligence services as are clandestine measures and everything that citizens experience as surveillance. In the case of school shootings, such measures have mostly been neglected in favour of more socially and community-oriented approaches. Not technology, but human factors have been identified as the major source of prevention.

It seems that communal self-organisation together with support from state agencies and research institutions are more successful than populist demands, whetted by industry, for more surveillance, new technologies or other security measures associated with terrorist attacks. Open environments such as schools have to be supported in their nature to be open. This in not to say that all has to be possible, but more restraints do not seem to be a way forward, rather they are arguably part of the problem.

3.5 THE OPEN NATURE OF DEMOCRACY: RESILIENCE AND VULNERABILITY

Professor Charles Raab and Dr Richard Jones, University of Edinburgh

The values of democracy

The subject addressed here requires some discussion of what is meant by 'democracy', before exploring the idea of the 'open nature of democracy'. It also requires a distinction to be drawn: between a democratic *political system* and a democratic *society*; and between procedural or institutional arrangements and the ethos or culture that underpins the society or political system. These matters have engaged sociologists, political scientists, psychologists and philosophers for centuries, and this is not the place to examine the enormous literature or the debates and controversies that have characterised thinking on this subject. However, it is important to note that political democracy comes in many varieties, with adjectival descriptors that indicate different dimensions and contexts in which the term has validly been used; using a range of standard sources, it is not difficult to compile a list of nearly forty varieties – not necessarily discrete – of democracy, and there are undoubtedly more.[810] There are, of course, many overlaps to varying degrees;

[810] Classical, Athenian, community, corporatist, representative, Madisonian, consociational, participatory, deliberative, pluralist, guided, juridical, parliamentary, proletarian, Rousseauian, party-

different labels are attached to very similar forms; some are general and others are specific; and the levels and domains in which they are held to operate vary.

This list, though long, is certainly incomplete, but there would be little point in going further if the aim of this section is to address the question whether democracy's 'open nature' makes it more resilient to, or more vulnerable to, threats that are made more likely through the exploitation of the opportunities afforded by these very values, or indeed through threats posed by those who seek to further their anti-democratic aims through clandestine or criminal activity. By no means, all of the adjectival 'democracies' listed above are characterised by a distinctly 'open nature', whether in the institutional and procedural forms that pertain to politics and governance, or in the texture of the society in which the political and governing system is situated. The question itself could also suggest that vulnerability varies directly with 'openness': the more open, the more vulnerable; but to validate that hypothesis would involve careful specification of terms and indicators as well as empirical evidence gathered and analysed through specific methods. This section can do neither; nor can it search for and cite scientific literature that addresses this proposition. It can therefore only give impressions and indications of these relationships insofar as they cast light on the main theme of the IRISS project. Understanding how *surveillance* threatens democracy is a further issue of importance, and is taken up at a later point.

We do not aim to define 'democracy', but to point to common denominators in most definitions. 'Government by the people' will do as an approximation.[811] This concerns the expression of the popular will, whether in choosing decision-makers or in deciding policies. In this vein, Haggerty and Samatas write:

> Democracy can succinctly, if not unproblematically, be characterized as power exercised by the people. Democracy involves a system of open procedures for making decisions in which all members have an equal right to speak and have their opinions count. …democracy is commonly associated with practices designed to ensure the fair and equitable operation of participatory decision-making. Ideally, it recognizes the interests of the majority while also trying to protect the concerns of the minority.[812]

The table below shows a number of key 'openness' values of democracy, identifies their contribution of value to social or political resilience and shows the typical threats

---

mediated, representational, tutelary, accountable, liberal constitutional, liberal, direct, indirect, people's equilibrium, social, socialist, one-party, multi-party, elitist, Schumpeterian, industrial, populistic, polyarchal, legal, developmental, radical developmental, competitive elitist, protective. The sources from which these terms are derived include: Holden, B., *Understanding Liberal Democracy*, Philip Allan, Oxford, 1988; Holden, B., *The Nature of Democracy*, Thomas Nelson, London, 1974; Held, D., *Models of Democracy*, Polity Press, Oxford, 1986; Held, D., and Pollitt, C. (eds.), *New Forms of Democracy*, Sage, London, 1986; Browne, M., and Diamond, P., (eds.), *Rethinking Social* Democracy, Policy Network, London, 2003; Hirst, P., *Associative Democracy: New Forms of Economic and Social Governance*, Polity Press, Cambridge, 1994; Duncan, G. (ed.), *Democratic Theory and Practice*, Cambridge University Press, Cambridge, 1983; Weale, A., *Democracy*, Macmillan, Basingstoke, 1999; Elster, J. (ed.), *Deliberative Democracy*, Cambridge University Press, Cambridge, 1998; Dahl, R., *A Preface to Democratic Theory*, University of Chicago Press, Chicago, IL, 1956.

[811] See Holden, B., *The Nature of Democracy*, Thomas Nelson, London, 1974, chapter 1, especially p. 8. For a discussion of definitional problems, see Held, D., *Models of Democracy*, Polity Press, Oxford, 1986, pp. 2-3.

[812] Haggerty, K., and M. Samatas, "Introduction – Surveillance and democracy: an unsettled relationship", in K. Haggerty and M. Samatas, (eds.), *Surveillance and Democracy*, Routledge, Abingdon, 2010, pp. 1-16, [pp. 1-2].

that make society and the political system more vulnerable to attacks on infrastructures and people by virtue of the operation and exercise of these values. The Table does not distinguish between infrastructures and people in identifying vulnerability; nor does it show nuances and subtleties in the identification of the relationship between value, threat and resilience, such as legal safeguards to prevent certain threats from being realised. The democratic values are considered on an abstract and idealised plane that might not correspond to the actual – and often less sanguine and more constrained – circumstances in which they operate. Nor are estimates given of the likelihood or magnitude of the threats (i.e., the degree of risk). In addition, 'resilience' is not defined here, nor is a distinction drawn between social, economic and institutional responses.

Open, democratic value	**Corresponding resilience value**	**Threat facilitated by open, democratic value**
Freedom of expression	Promotes democratic debate; values individual expression; promotes new ideas; adds to stock of ideas; promotes ideological pluralism; prevents capture of the public sphere by any single wilful group.	Hate speech; abandonment of reasoned discourse; manipulative persuasion; undermining of truthful communication.
Freedom of information, transparency, and accountability	'The truth will out'; disperses information across society; is necessary for an informed citizenry; exposes corruption and poor performance.	Misuse of information, causing specific harms to certain individuals or groups; state security can be compromised by the exposure of certain state services to public gaze.
Privacy	Protects individuals' private lives; promotes their ability to form social and political relationships.	Might be used to conceal criminal/subversive activity, plans, conspiracies, etc.
Freedom of movement	Protects self- or group fulfilment; promotes relationships and hence contributes to social capital; promotes personal and group autonomy; promotes political expression	Terrorism; espionage; conspiratorial connections.
Freedom of assembly	Promotes political expression; facilitates resistance; promotes participation; sustains non-conformity and a counter-culture.	Misuse of public places; intimidation of certain individuals or groups.
Rule of law	Checks against arbitrary exercise of authority.	Formal protection to freedoms, but still allows substantively illiberal laws; the mere semblance of legality; protection of the rights of those who attack democracy or commit crimes.
Freedom of communication	Expression of a variety of heterodox ideas; contributes to social and personal capital; facilitates planning and co-ordination.	Conspiracies of various kinds conducted through uncensored and unmonitored communication channels.
Freedom of religion	Liberty of conscience; can promote plurality; tolerance.	'Extremism', with tendencies towards harmful activity.
Freedom of self-determination	Promotes societal flexibility.	Increases likelihood of public disorder and conflict between groups or individuals.

Table 1 Democratic values, resilience and threats

The above table draws and expands upon a smaller version drafted for this Deliverable on 10 May 2013 by Trilateral and IRKS, which was further elaborated by the University of Edinburgh on 8 October 2013 for presentation at a Consortium meeting on 16-17 October 2013.

Liberal democracy best sums up the type of political democracy that is based on these ideals. It occupies a position that is high on a spectrum of openness that ranges from deliberative democracy, which maximises popular rule in a large swathe of decision-making throughout society and the polity; to elitist or Schumpeterian democracy, which relegates popular participation to a periodic choice among competing teams of rulers aiming to run the country. However, even at the 'low' end, the inventory of freedoms and rights given in the above table, might be constitutionally entrenched and sustained in practice; if they were not, the country's enjoyment of the label 'democracy' would be in question.

A further value often associated with democracy is *equality*, both as a condition of democracy and as a criterion of the degree of democracy exhibited in particular institutions and processes.[813] Social and economic equality have become part of the conventional understanding of what a democratic *society* should be like, or have been seen as necessary for (political) democracy. Democracy is often held to be inconsistent with marked discrepancies of class, caste, and social or economic status, such that 'democratic society' connotes a (more or less) egalitarian distribution of things that are valued. 'One person, one vote' and 'one vote, one value' are hallmarks of political democracy; apart from voting, political democracy requires that there be no, or low, barriers to participation (e.g., voting, office-holding, influence) and that the ability to participate should be distributed equally across society.

The countries of the European Union (EU) profess a form of democracy that most closely approximates liberal democracy in terms of their openness, their subscription to the values inherent in the freedoms and rights we have identified, and processes of politics and government in which a high degree of transparency and accountability are evident. This is not to say that these criteria are fulfilled in practice, but that they form the basis of legitimacy for these states, and even serve as qualifications for membership in the EU. Indeed, in these countries, criticism of regimes is often based on the shortfall or failure in practice to live up to these conditions or to enforce rules that support them: for example, the curtailment of freedoms of expression or assembly, electoral corruption or unfairness, or arbitrariness and administrative discrimination in place of the rule of law. The existence of laws and regulatory agencies, as well as of vigilant civil society bodies and a free press (or other media), are hallmarks of liberal-democratic political systems.

[813] Held writes, "Democracy entails a state in which there is some form of *political equality* among the people". Held, D., *Models of Democracy*, Polity Press, Oxford, 1986, p.2; emphasis in original.

Table 1 suggests that vulnerability is the obverse side of the coin of strength: what gives democracy its essential and attractive quality is also what enables some to take advantage of freedoms, rights and liberties in ways that pose a threat to these very values. This may occur through the misuse of open, democratic processes, rights and freedoms by individuals or movements towards which democratic values require tolerance as legitimately 'within the pale' of democratic politics and society, up to the point where they demonstrably constitute what some would call a 'clear and present danger' of undermining that society or system. More ominously, however, the threat may come from covert plots and conspiracies 'beyond the pale' that flourish in the tolerant climate of democracy but that, if their aims are achieved, would replace democracy with other kinds of system that are antithetical to it. Some forms of terrorism provide an example of clandestine activity that aims to subvert democratic values and practices and to supplant them by non-democratic, authoritarian or 'closed' ones, and to transform the open quality and texture of everyday life.

Words to the effect of 'the price of liberty is eternal vigilance' are well known, if difficult to attribute, but it seems apt to apply them to democracy. They underscore the dilemma or paradox of democracy: that the philosophical and ethical principles that it represents might not withstand challenges that test their viability without deploying specific kinds of defence – in the name of democracy or of the security of a society or entity – that could include surveillance of such an extent and intensity that democracy itself is contradicted. In that case, the question – or dilemma – is how democratic politics and society can remain true to their values whilst at the same time defeating their opponents, especially those whose activities put them beyond the pale. As the IRISS project shows, the analytic frame thus shifts from considering surveillance as a resilience practice in the face of threats, to considering how societies can be resilient to that surveillance itself where it becomes a significant threat. The values of democracy might or might not provide the means for such resilience.

Democratic political systems

A range of rights and freedoms can be linked to democracy on the normative and conceptual plane as ideals, albeit not always empirically. This range includes freedom of expression, freedom of information, freedom of movement, freedom of assembly, freedom of communication, privacy, and the rule of law.

Let us look a bit more closely at democracy's values. Citing the *Stankov* case,[814] Hallinan states:

> Freedom of expression essentially protects the right to express oneself and the means one chooses to do it, while freedom of association and assembly protects the right to share one's beliefs or ideas, and to act in a public capacity, in community with others. The centrality of these rights to the European concept of democratic society has been repeatedly clarified by the

[814] Hallinan quotes the Court's statement in *Stankov*. "The essence of democracy is its capacity to resolve problems through open debate. Sweeping measures of a preventive nature to suppress freedom of assembly and expression other than in cases of incitement to violence or rejection of democratic principles – however shocking and unacceptable certain views or words used may appear to the authorities, and however illegitimate the demands made may be – do a disservice to democracy and often even endanger it. In a democratic society based on the rule of law political ideas which challenge the existing order and whose realisation is advocated by peaceful means must be afforded a proper opportunity of expression through the exercise of the right of assembly as well as by other lawful means." ECtHR (1st sect.), *Stankov a.o. v. Bulgaria* (Appl. No. 29221/95), judgment of 2 October 2001, para. 97.

> European Court of Human Rights (ECtHR) in its affirmation of the direct links between them and democracy and pluralism.[815]

He argues that these rights help to constitute a 'public sphere', to strengthen the bonds and individual capacities within it, and to form a boundary with the state. Arguments for freedom of information, communication and assembly are typically framed in terms of their centrality to a democratic polity that enshrines transparency for its dealings and values public enlightenment. Likewise, the 'private space' – which is not in contradiction to the idea of a 'public sphere' – that is safeguarded by privacy is argued to be a condition of democracy.[816] The rule of law safeguards all these freedoms and rights by providing an underpinning of certainty, non-arbitrariness, legitimacy, and the legal conditions for the working of democratic institutions. It also stands in opposition to measures – whether procedural or substantive – that would constrict the exercise of freedoms and rights.

Crucially, then, the workings of a democratic political system depend upon the (equal) freedom of people to communicate with each other, to assemble, to move physically about the state's territory, and to 'move' virtually round the Internet in search of opinions and information. As noted earlier, they also require (the right to) privacy as a means of securing autonomy, providing individuals – again, on an equal basis – with a zone in which they can prepare to forge social and political relationships and engage with the public sphere. The rule of law serves as a guarantor of all these values.

Insofar as liberal-democratic polities require a substantial level of freedoms and rights in practice beyond what is minimal or nominal, the range of vulnerability might be wide. It can be argued that the more the criteria of liberal democracy are in place, and the greater the range and depth of their institutional buttressing and the existence of the means of criticism and opposition, the more vulnerable might these democracies be to threats and attacks from within and without. Covertly planned, anti-democratic terrorism might suspend or erode these freedoms through intimidation. The breakdown of public order, or physical disruption, might prevent the realisation of certain freedoms. Media monopolisation might attack the availability of dissenting views or of information, which play an essential part in helping to create an informed and critical citizenry and to shape public will prior to voting or deciding.

Institutions and procedures of democracy are not all unique to liberal democratic polities, and the latter's vulnerability to attacks of various kinds might be common to that experienced by other kinds of polities' institutions and procedures. Physical attacks on political and governmental actors (e.g., those who work in legislatures, executives and the judiciary) might threaten democracy (or indeed, even non-democracies), and cyber-attacks might cripple institutions and infrastructures that are crucial for governance. Currently, a great deal of attention and resource investment occurs in many countries in order to be resilient to this source of vulnerability. Moving nearer to the realm of more 'open' and participatory practices involving the general public and not just office-holders, and where elections take place to constitute a legislature and part of the executive, electoral processes are prone to disruption through sabotage, corruption, and technical malfunctioning. Attacks on the integrity of

[815] Hallinan, D., "Effects of surveillance on freedom of assembly and association, and on freedom of expression", in D. Wright, and R. Kreissl, (eds.), *Surveillance in Europe,* Routledge, London, forthcoming. This book is based on IRISS deliverable D.1.

[816] Raab, C. and B. Goold, *Protecting Information Privacy*, Research Report 69, London: Equality and Human Rights Commission, 2011, p. 18; Goold, B., "Surveillance and the Political Value of Privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009; Raab, C., "Surveillance: Effects on Privacy, Autonomy and Dignity", in D. Wright, and R. Kreissl, (eds.), *Surveillance in Europe,* Routledge, London, forthcoming.

democratic elections are also therefore a subject for resilient strategies involving staff training, public education, equipment improvement, vigilance, and criminal sanctions: in other words, precautions, preventions and remedies.

Democratic societies

It is less clear how the question about the vulnerability of the openness of democracy should be answered for democratic *societies* – where the quality of social life is at issue – apart from the political system, where the focus is on institutions and processes for governance. A democratic society requires respect for, and the exercise of, these same freedoms and rights. But while the discussion of a democratic political system centred upon the part these values play in the relationship between the people and the state within various kinds of political democracy, and in particular for liberal democracy, for a democratic society the canvas is wider still. A democratic society – albeit ideals and reality might well diverge on this – can be portrayed as one in which people are free to act and live their lives as they wish, singly or in groups, as long as they do so within laws that are not arbitrary and with tolerance and respect for the rights of others to do so. It is also a society in which people have wide latitude to develop their autonomous personalities, to pursue their interests and projects, and to form social relationships to the maximum degree consistent with the possibility for others to do likewise, and not to have to seek permission from 'authority' to engage in these self-developmental activities. Social and individual behaviour is fluid, not regimented, and in practice the heterogeneity of society does not necessarily increase the likelihood of social conflict; or when conflict arises, has no resources for reconciling differences rather than suppressing them through authoritarian imposition.

'Democratic society' also indicates the nature of relationships within and between the associations and other formations that constitute the society at whatever structural level – e.g., national; local; civil society bodies such as trade unions, cultural or ethnic bodies, and religious groups – as well as the decision-making processes, if any, that take place in these constituent parts. Here, the assumptions about equality are also germane insofar as democracy and equality are considered to be linked values. The price of pluralism might be the toleration of arrangements in social groups based on consent or voluntary membership that sustain practices that contradict one or more democratic values.[817] Thus the persistence of inequalities of all kinds in complex contemporary societies that call themselves 'democratic' reflects the tension between ideal and reality. The 'open nature' of such societies is heavily qualified by the differential enjoyment of freedoms, rights and liberties that belie the formal equality that may exist in legal and rhetorical discourse.

Democratic societies can be as vulnerable to attacks on their open nature as are democratic political systems. The freedoms and rights enjoyed by the infrastructures, groups and individuals of a democratic society – here considered apart from their political role – might be restricted or undermined by similar kinds of threat as those that interfere with the workings of politics and government.

Surveillance and resilience

At this point, however, it is important to consider the way in which the resilience strategies undertaken by the state or society in the face of threats – some of which are made more

[817] For example, non-egalitarian religious or educational organisations, or exclusive private clubs.

prevalent through the 'open nature' of democracy – might entail activities that attack that very open nature in the name of security and safety, as mentioned earlier. Ostensibly protecting democratic freedoms and rights, resilience measures – perhaps especially those that involve *surveillance* – might themselves lead to a more closed society that brings democracy into question. If we take the public sphere as a property of democracy, we can understand how (state) surveillance poses a threat to its functioning and integrity. Amicelle has shown the implications of security-oriented surveillance and 'traceability' on freedom of movement.[818] The 'private space' that is maintained by privacy as a condition of democracy can be threatened by surveillance. The 'chilling effect' of surveillance – and perhaps especially covert *mass* surveillance of the kind made apparent by the Snowden revelations in 2013 – also potentially threatens not only the practice of freedoms and rights, but social relationships as well. The intimidation or proscription of civil society bodies, either by terrorism or state surveillance, bodes ill for democratic society as well as for liberal political democracy; so too might preventative action (e.g., policing) aimed at reducing the likelihood of disorder and disruption.

To the extent that a democratic society or polity requires certain egalitarian conditions to be met, it is possible to recognise threats to their achievement. Whether surveillance threats to social equality can be similarly identified is less certain, although social sorting is a prime candidate:[819] its discriminatory effects – preferment and disadvantage – can be theorised as detracting from the democratic quality of the society just as it does for the political system. Referring to 'differential control' surveillance systems that are applied disproportionately to the poor, ethnic minorities, or women, Monahan writes:

> If social equality and equal participation (or representation) in governance processes are necessary conditions for strong democracy, then systems that perpetuate social inequalities are antidemocratic.[820]

Control over the design and use of public space – real or virtual – that feature prominently among surveillance practices might interfere with freedom of movement and freedom of assembly, whether deliberately or as a by-product of over-riding criteria for creating secure, functional, efficient, or profitable transport, buildings, streets, shopping malls, the Internet, and the like. An effect of 'dataveillance' and profiling, for example, is to enable the targeting of groups or individuals as 'suspicious'. This, in turn, might make the targeted feel persecuted and isolated, thus making it more difficult for them to enjoy the benefits of democracy. Depending on how it is implemented, even lawful and statutorily supported surveillance can have repercussions on the rule of law.

In the face of these and other threats, the values of democratic society and politics provide structural and normative resources for resilience. For example, democratic politics provide scope for multiple interest groups and associations to identify threats and to plan and co-ordinate responses so that society can continue to function. The existence of myriad groups

---

[818] Amicelle, A., "Surveillance and freedom of movement", in in D. Wright, and R. Kreissl, (eds.), *Surveillance in Europe,* Routledge, London, forthcoming.

[819] See, for example, Lyon, D. (ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, Routledge, London, 2003; Bowker, G. C. and S. L. Star, *Sorting Things Out: Classification and its Consequences*, The MIT Press, Cambridge, MA, 1999; Ball, K., Haggerty, K. and Lyon, D. (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, Abingdon, 2012, Part II.

[820] Monahan, T., "Surveillance as governance: social inequality and the pursuit of democratic surveillance", in K. Haggerty, and M. Samatas, (eds.), *Surveillance and Democracy*, Routledge, Abingdon, 2010, pp. 91-110, [p. 97].

and arenas in which free debate and the habits of civic participation are cultivated and widely distributed provides cultural and behavioural resources for defending a democratic way of life against attempts to close it down. Similarly, the instruments available in constitutions, laws and political and judicial procedures can be seen as tools for resilience by legitimising measures for anticipating or responding to threats posed by surveillance. They also provide guidelines – albeit contested – for determining and overseeing the boundary between legitimate challenges to the workings of democratic politics and society and challenges that either aim to undermine the latter or that would have that effect. In these and other ways, the values of democracy are not just philosophically cogent and admirable, but they also provide practical defences for the polities and societies in which they are proclaimed and embodied.

4 RESILIENCE IN A SURVEILLANCE SOCIETY

David Wright, Trilateral Research & Consulting LLP
Dr Reinhard Kreissl, Institute for the Sociology of Law and Criminology (IRKS)

This section first defines and characterises a "surveillance society". While surveillance can be used to protect society from criminals and terrorists, ubiquitous (or mass) surveillance can undermine the very freedoms and values it aims to protect. It then (based on the analysis in the preceding parts of the deliverable) examines in particular, resilience in a surveillance society, and whether resilience offers a useful strategy for countering the negative effects of surveillance in undermining the freedoms and values that underpin a democracy.

4.1 DEFINITIONS OF "SURVEILLANCE SOCIETY"

The term "surveillance society" is hardly a new one. It already had currency by the mid-1990s. David Lyon, one of the leading surveillance studies scholars, used the term in the subtitle of his 1994 book *The Electronic Eye*.[821]

Oscar H. Gandy used the term the year before in his book *The Panoptic Sort*,[822] and even earlier in the title of an article he published in 1989,[823] the same year in which David Flaherty published his book, *Protecting Privacy in Surveillance Societies*.[824] Four years before this, in 1985, Gary T. Marx wrote an article for *The Los Angeles Times* in which he described how the "categorical monitoring" associated with new technologies "is creating a society in which everyone, not just those that there is some reason to suspect, is a target for surveillance".[825]

Marx seems to have coined the term some months earlier in his 1985 publication: "The surveillance society: the threat of 1984-style techniques" in *The Futurist*. That paper was prescient. It stated, "Recent developments in surveillance technology permit intrusions that

[821] Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*, Polity Press, Cambridge, UK, 1994.
[822] Gandy, Oscar H., *The Panoptic Sort: A Political Economy of Personal Information*, Westview Press, Boulder, CO, 1993.
[823] Gandy, Jr., Oscar H., "The surveillance society: Information technology and bureaucratic social control", *Journal of Communication*, Vol. 39, No. 3, Summer 1989, pp. 61-76.
[824] Flaherty, David, *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, 1989.
[825] Marx, Gary T., "We're all under surveillance", *The Los Angeles Times*, 1 Dec 1985.
http://web.mit.edu/gtmarx/www/all_under_surveillance.html

were once the realm of science fiction."[826] It accurately predicted that "People may gladly consent to the monitoring of their behavior. Information may be willingly given to a data bank in order to obtain consumer credit or some benefit (welfare, driver's license) with no concern about how the information will be used or who will have access to it....Surveillance may be welcomed because it is benignly presented as a means to protect people from crime."[827] It also warned,

> The gigantic data banks that computers have made possible offer an efficient means to store, retrieve, and analyze personnel information. Thus, they encourage the creation and retention of data that in the past would not have been collected or saved. They make possible dossiers on a scale that was previously unimaginable and weaken the position of the individual relative to large organizations capable of assembling and analyzing these data.[828]

It further noted,

> Today's surveillance technology can prod ever deeper into physical, social, and personal areas....The categorical monitoring associated with video cameras, metal detectors, electronic markers on consumer goods and even library books, and the computer are creating a society in which everyone, not just a few suspects, is a target for surveillance.... surveillance technology makes privacy much more difficult to protect.[829]

So many of the features and issues of a modern surveillance society were already visible, at least to Marx, almost 30 years ago – not only the technologies and practices, but also the "categorical monitoring" (a term which would morph into "social sorting"). He foresaw that people would accept or even welcome some measure of surveillance in exchange for convenience or perceived protection. What seemed like a dark dystopian scenario some 30 or 40 years ago, has become a pervasive element of everyday life in present day societies. A movie like *Fahrenheit 451* by the French filmmaker Francois Truffaut released in 1966 and based on the novel from science fiction writer Ray Bradbury today looks almost like a prophetic documentary of present-day societies. Intended as an artistic narrative of what could be termed forced consumerist obedience, the society projected in this movie has become reality today. Orwell's dystopian vision has come through, though with a different twist.

Although all of the above are noteworthy publications, undoubtedly the term 'surveillance society' came into widespread use, at least in Europe, with publication of a report produced for the UK Information Commissioner in 2006. Based on that report, then Commissioner Richard Thomas warned in August 2006 that the UK was "sleepwalking into a surveillance society",[830] by which he meant not only that surveillance was becoming ubiquitous in the UK, but that most people were unaware of its ubiquity, that there was little public debate about its ubiquity and its effects, and how negative effects could be countered.

The report, prepared by the Surveillance Studies Network (SSN), stated that "massive surveillance systems… now underpin modern existence" and that "these systems represent a basic, complex infrastructure which assumes that gathering and processing personal data is

---

[826] Marx, Gary T., "The surveillance society: the threat of 1984-style techniques", *The Futurist*, June 1985, pp. 21-26 [p. 23].
[827] Ibid.
[828] Marx, op. cit., 1985, p. 24.
[829] Marx, op. cit., 1985, p. 26.
[830] Booth, Jenny, "UK 'sleepwalking into a Stasi state'", *The Guardian,* 16 August 2004. http://www.theguardian.com/uk/2004/aug/16/britishidentity.freedomofinformation

vital to contemporary living". It said that "the surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy. Surveillance may be viewed as progress towards efficient administration."[831] While the SSN saw the surveillance society as an outcome of modern organisational practices, the Snowden revelations show today's surveillance society in an entirely different light – highlighting the "covert conspiracy" that the SSN dismissed.

The SSN report defined surveillance as follows: "Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance."[832] It added that "The collection and processing of information about persons can be used for purposes of influencing their behaviour or providing services."[833] But surveillance is more than that. Intelligence agencies and probably some companies not only use surveillance to discover what their enemies are doing, but also uncover the activities of their competitors, and even their "friends" and allies.

In a UK House of Commons Home Affairs Committee report on surveillance prepared two years after the ICO report, the authors defined surveillance as "as a term that encompasses not only the use of monitoring and recording technology but also the creation and use of databases of personal information and the record of our communications in the digital age".[834] This seems closer to current practice where, in Europe, the Data Retention Directive obliges communications providers to retain customer metadata ("the record of our communications") for between six months and two years.

The Home Affairs Committee report exhorts the government to be careful otherwise we might end up in a surveillance society: "The potential for surveillance of citizens in public spaces and private communications has increased to the extent that ours could be described as a surveillance society unless trust in the Government's intentions in relation to data and data sharing is preserved."[835] The Home Affairs Committee seems to regard the presence of trust as a distinguishing feature of what is and is not a surveillance society. However, many would argue that we are already in a surveillance society and that trust has been damaged, perhaps beyond repair, as we discover how pervasive surveillance has become. Trust is built on transparency, and governments and companies have generally not displayed either in regard to the extent of surveillance or the purposes of many of their surveillance systems.

Soon after the House of Commons report, the House of Lords produced its own report, which distinguished two broad types of surveillance: mass surveillance and targeted surveillance. It describes mass surveillance as "passive" or "undirected" surveillance. It does not target any particular individual but gathers images and information for possible future use. CCTV and databases are examples of mass surveillance.[836] The Snowden revelations and what we know

---

[831] Surveillance Studies Network (SSN), *A Report on the Surveillance Society*, For the Information Commissioner, September 2006, p. 1.
[832] Ibid.
[833] SSN, op. cit., 2006, p. 4.
[834] House of Commons Home Affairs Committee, *A Surveillance Society?*, Fifth Report of Session 2007–08, Volume I, The Stationery Office, London, 8 June 2008, p. 11.
[835] Ibid., p. 12.
[836] House of Lords Select Committee on the Constitution, House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, Volume I: Report, 2nd Report of Session 2008–09, The Stationery Office, London, 6 Feb 2009, p. 12.

about surveillance by social networks have shown us that we have moved into an era of mass surveillance. That is the norm today.

Monahan distinguishes two types of surveillance that

> directly challenge ideals of democratic governance. These are systems of *differential control* and *automated control*, the effects of which are most egregious when the systems coexist or are one and the same. Differential control can be witnessed first with the 'social sorting' functions of surveillance systems (Lyons, 2003, 2007). Surveillance, in this regard, operates as a mechanism for societal differentiation... If social equality and equal participation (or representation) in governance processes are necessary conditions for strong democracy, then systems that perpetuate social inequalities are antidemocratic.... Automated control depends predominantly upon algorithmic surveillance systems, which take empirical phenomena – translated into data – as their raw material, ranging from commercial purchases to mobility flows to crime rates to insurance claims to personal identifiers. Spaces, activities, people, and systems are then managed through automated analysis of data and socio-technical intervention... Automated control systems share a predictive orientation toward people... the systems seek to fix identities in advance for more effective control, regardless of the questionable ethics associated with acting on predictions.[837]

If such types of surveillance can be easily found in today's society, does it mean that we do not live in a democracy? If surveillance underpins society today, how would we characterise the type of society in which we live? Bart Jacobs distinguishes surveillance society from totalitarian society, but the distinction is somewhat fuzzy:

> Surveillance societies have mechanisms for monitoring, influencing and controlling people in their private lives. These mechanisms may be used for commercial, political or security reasons. In case the authorities actively use these mechanisms to monitor, influence and control people in their private lives on a large scale, the term 'totalitarian society' will be used.... deliberately exerting explicit influence and control in private lives is considered part of the idea of a totalitarian society, not of a surveillance society. One may argue that a transformation of a surveillance society into a totalitarian society is primarily a matter of politics, not of technology.[838]

Jacobs seems to distinguish between a surveillance society and a totalitarian society by virtue of "deliberately exerting explicit influence and control".[839] Such as distinction rests on a concept of democratic governance that probably no longer provides adequate tools for analysing the modes and strategies operative in modern societies. While the institutional outfit of these societies displays all features of a democratic polity, democracy has been hollowed out. We are living, as Colin Crouch puts it, in a post-democracy.[840] Following the line of reasoning developed in the tradition of a Foucauldian social analysis, the dominant mode of governance in these societies is – using a term from Rose and Miller – governing through freedom.[841] With this fundamental shift in the structure of modern societies, the distinction between totalitarian and liberal societies is about to become, at least from a theoretical

---

[837] Monahan, Torin, "Surveillance policies and practices of democratic governance", in Kevin D. Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, Abingdon, 2010, pp. 91-110 [pp. 97-98].
[838] Jacobs, Bart, "Keeping our Surveillance Society Non-Totalitarian", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009, pp. 19-33 [p. 19]. http://ojs.ubvu.vu.nl/alf/issue/view/14
[839] Ibid.
[840] Crouch, Colin, *Post-democracy*, Polity, Cambridge, 2005.
[841] Nikolas, Rose, and Peter Miller, "Political Power beyond the State: Problematics of Government", *The British Journal of Sociology*, Vol. 43, No. 2, June 1992, pp. 173-205.

perspective obsolete. Present day societies are surveillance societies, but using the analytical distinction between totalitarian and pluralist or liberal does not help here since surveillance cuts across this difference.

Following Jacobs, one could argue that today's surveillance society already is a totalitarian society, because both governments and large companies, such as Google and Facebook, are definitely deliberately exerting explicit influence and control. They are tracking everyone, just as the NSA and GCHQ are doing, and aiming to turn everyone into consumers of their services and the advertising they generate. There are similarities with a totalitarian society, but periodic elections seem to belie such a characterisation. With its elections, our society is perhaps akin to that depicted in Spielberg's film *Minority Report*. In that film, there are elections but surveillance is also rampant, with targeted advertising, preventive crime control, optical access control and various other surveillance technologies.

As Nils Zurawski points out, defining surveillance means more than technologies.[842] He contends that surveillance describes a field or process involving actors, policies, technical measures, ideologies, laws and regulations. Surveillance emerges out of the relations between two or more of these aspects, not necessarily good or bad (which is a moral question). He argues that the question of how society can be resilient to surveillance presupposes that surveillance is always irritating. We need to pay attention to the ways in which surveillance is to be implemented by new laws and how surveillance technologies impact on society and whether this enables society and its members or inhibits them from doing something. Surveillance may impact rights or enable citizens to exercise a right. Surveillance may invade their privacy or generate transparency about the State's activities. He argues that we should not be misled by the technological connotation and the images that are generated by the word surveillance and the iconic camera. An open-minded approach is important in evaluating resilience measures, as being resilient to a camera means something entirely different to being resilient to a certain policy with its norms or norm-generating effects.[843]

The authors of this section have synthesised various definitions of and perspectives on a surveillance society to produce an overarching definition as follows:

> A surveillance society is one in which the use of surveillance technologies has become virtually ubiquitous and in which such use has become widely (but not uniformly) accepted by the public as endemic and justified by its proponents as necessary for economic and security reasons. Even if there are democratic procedures, a surveillance society is one in which there is a parallel system of power exercised by large, oligarchic companies and intelligence agencies over which effective oversight and control are largely illusory.

In the next section, we identify various manifestations of the surveillance society.

4.2 MANIFESTATIONS OF TODAY'S SURVEILLANCE SOCIETY

Among the manifestations of today's surveillance society are the following:

Citizen-consumers contribute to their own surveillance by exchanging their personal data for some perceived benefit or service. As almost no one reads privacy policies or terms and conditions for online services, which are incomprehensible for the lay person anyway, citizen-

[842] E-mail from Nils Zurawski, 2 Sept 2013.
[843] Ibid.

consumers trade away vast amounts of their personal data without knowing the extent to which they are doing so.

Facebook and other social media are examples of "participatory surveillance", where people contribute the personal data that allows them to be surveilled, socially sorted and targeted with personalised advertising. Roger Clarke coined the term "dataveillance" to describe the phenomenon of people being surveilled as they use data networks (notably, the Internet).

The "biggest" surveillants (i.e., those that are able to conduct truly mass surveillance) are governments and companies, but the declining costs of surveillance technologies put those technologies into the hands of many other players, including local authorities and even one's neighbours.

In today's surveillance society, some governments not only surveil (spy on) criminals and terrorists, but also everyone, including their allies, as has become amply apparent from the Snowden revelations. Intelligence agencies such as the NSA, GCHQ and others such as those of China and Russia not only engage in surveillance, but also in cyberattacks and propaganda designed to "destroy, deny, degrade [and] disrupt" enemies.[844]

There is a vigorous, rapidly growing industry feeding the ubiquity of surveillance, as detailed in the Statewatch NeoConOpticon report[845] and a chapter on the surveillance industry in the volume on surveillance in Europe.[846]

A characteristic of today's surveillance society is the use of "smart surveillance", assemblages that greatly leverage the use of individual technologies. Smart surveillance is sometimes known as algorithmic surveillance, because it generates digital data that can be automatedly analysed.

Another manifestation of the surveillance society is mining of data from diverse sources, into an assemblage frequently referred to as "Big Data".

A hallmark of a today's surveillance society is the lack of transparency and secret orders such as those given to telecom companies not to reveal the extent to which the traffic on their networks are under surveillance. Edward Snowden highlighted the dangers to democracy from a lack of transparency. In February 2014, he told students at Oxford University (via a video link) that "The foundation of democracy is the consent of the governed. After all, we cannot consent to programmes and policies about which we are never informed. The decline of democracy begins when the domain of government expands beyond the borders of its public's knowledge."[847] David Lyon has made somewhat similar criticisms of the lack of transparency, "the codes by which persons and groups are categorized are seldom under public scrutiny (and if they related to 'national security' they may well be veiled in official

[844] Cole, Matthew, Richard Esposito, Mark Schone and Glenn Greenwald, "Snowden Docs: British Spies Used Sex and 'Dirty Tricks'", *NBC News*, 7 Feb 2014. http://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091

[845] Hayes, Ben, *NeoConOpticon: The EU Security-Industry Complex*, Statewatch and the Transnational Institute, London, June 2009. http://www.statewatch.org/analyses/neoconopticon-report.pdf

[846] Rodrigues, Rowena, "The surveillance industry in Europe", in D. Wright, and R. Kreissl, (eds.), *Surveillance in Europe,* Routledge, London, forthcoming.

[847] Smith, Lewis, "Edward Snowden tells Oxford students that Government secrets undermine democracy", *The Independent,* 20 Feb 2014. http://www.independent.co.uk/student/news/video-edward-snowden-tells-oxford-students-that-government-secrets-undermine-democracy-9139897.html

secrecy) and yet they have huge potential and actual consequences for the life chances and the choices of ordinary citizens."[848]

Yet another hallmark is the vengeful, arbitrary, surveillant government that does not like its surveillance practices uncovered, that will go to extraordinary lengths in its attempts to capture whistle-blowers, as the United States did when it asked European governments not to allow the overflight of the Bolivian president's plane when it took off from Moscow amid suspicions that Edward Snowden might be aboard.[849] Governments hunt and punish whistle-blowers unrelentingly. They also hassle the journalists and their newspapers, as the UK did when it detained under anti-terror laws David Miranda, partner of *Guardian* journalist Glenn Greenwald, for nine hours in August 2013 when he changed planes at Heathrow on his way from Berlin to his home in Brazil and police seized electronic items. The security services also tried to bully *The Guardian* from publishing more leaked material from Edward Snowden. GCHQ sent two operatives to *The Guardian*'s offices to oversee the destruction of computer hard drives said to contain leaked information.[850]

Another feature of a surveillance society is the message from authorities to report not only suspicious packages but also suspicious behaviour.[851]

Surveillance also permeates our culture, as evidenced by films such as *The Conversation*, *The Net*, *Enemy of the State*, *Minority Report*, *The Truman Show*, etc., and TV programmes such as *Big Brother*, *Person of Interest*, etc. Popular culture, especially the TV series such *Big Brother*, help to make people think that surveillance is not only acceptable and a normal part of everyday life, but also fun. Others such as *Enemy of the State* serve as warnings.

Although one can distinguish different types of surveillance – dataveillance and panoptic surveillance (the few watch the many), synoptic surveillance (the many watch the few, e.g., via the news media or Big Brother TV series), sousveillance (lifelogging: an individual records her participation in an activity[852]), überveillance (an omnipresent electronic surveillance facilitated by implants in the body), participatory surveillance (people participate in their own surveillance by supplying personal data to a social network), rhizomatic surveillance (interconnected surveillance systems), etc. – surveillance today is dominated by the surveillance activities of the state (NSA, GCHQ, etc.) and large corporations (Facebook, Google, etc.). This spread of surveillance, facilitated by improved technologies makes the tracking, locating and social sorting of citizens appear like a quasi-natural fact of modern life. Confronted with critical assessments of side effects and shortcomings the standard response from political representatives falls back on a rigid ideological position. Like the infamous

---

[848] Lyon, op. cit., p. 32.

[849] Shoichet, Catherine E., "Bolivia: Presidential plane forced to land after false rumors of Snowden onboard", *CNN,* 3 July 2013. http://edition.cnn.com/2013/07/02/world/americas/bolivia-presidential-plane/index.html

[850] Alan Rusbridger, the newspaper's editor, said that *The Guardian* did not accept UK Prime Minister Cameron's accusation and that its position had been misrepresented. "We went along with the destruction of the computers in the knowledge that we could carry on reporting from New York," he said. Cowell, Alan, "Cameron Criticizes The Guardian for Publishing Secrets", *The New York Times*, 16 Oct 2013. The event is detailed in Harding, Luke, *The Snowden Files: The Inside Story of the World's Most Wanted Man*, Guardian Books and Faber and Faber, London, 2013, pp. 171-193.

[851] Marx, Gary T., "The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes", *IEEE Security & Privacy*, Sept-Oct 2013, pp. 56-61 [p. 58].

[852] Sousveillance can also mean surveillance by the surveilled of authorities, e.g., protesters recording the actions of police during a demonstration. Sousveillance in this sense is sometimes called reverse or inverse surveillance. See Clarke, Roger, "The Regulation of Civilian Drones' Applications to the Surveillance of People", Xamax, 2014. http://www.rogerclarke.com/SOS/Drones-BP.html

TINA-approach introduced by the late Margaret Thatcher (TINA= There Is No Alternative) politicians refuse to have second thoughts about encompassing surveillance. It is interesting to note that in today's surveillance society, a young, idealistic political neophyte such as Barack Obama, who spoke out against surveillance when he was a freshman Senator, became a convert to ubiquitous surveillance once he became president.[853]

Governments and companies use surveillance for various purposes. In *Privacy in Peril*, James Rule reviews surveillance in several countries, including the UK. He comments that

> Britain has evolved into a world of pervasive everyday surveillance… British law permits a wide range of investigators to monitor contents of communications – from letters to telephone conversation and e-mail messages – without court order. Such monitoring is possible for a sweeping array of purposes, as specified under the Regulation of Investigatory Powers Act of 2000:
>
> (a) In the interests of national security
> (b) For the purposes of preventing or detecting serious crime
> (c) For the purpose of safeguarding the economic well-being of the United Kingdom; or
> (d) For the purpose… of giving effect to the provisions of any international mutual assistance agreement.
>
> Note the openness of these purposes – especially (b). Since prevention applies to crimes that have not yet occurred, authorities are encouraged to imagine which communications could culminate in crimes perhaps not yet contemplated even by the hypothetical perpetrators.[854]

Rule points out that the UK was the major driving force behind the EU's Data Retention Directive, which requires Member States to adopt legislation requiring storage of communications metadata for periods ranging from six months to two years.[855] Following his review of surveillance practices in the US, UK, Australia, Canada and France, Rule concludes that

> the evolution of government surveillance… entails a profound shift in what one might call the *ecology* of personal data… governments are gaining access to more different kinds of information on people's lives. And they are fashioning more efficient checkpoints where such data can be brought to bear in forceful decision making on the people concerned. The net effect of these developments is to broaden the coverage of ordinary people's everyday lives through mass surveillance – and thereby extend the forms of compliance that governments can expect from their people.[856]

As Coleman and McCahill point out, however, the reach of surveillance is uneven. While surveillance might be helpful in prosecuting street crime, it is not much used to apprehend corporate criminals.[857] Some people are more surveilled than others. Those seeking benefits from the State's social system are arguably more surveilled than those who commit and appear to get away with corporate crimes. Surveillance reinforces asymmetries of power.[858]

---

[853] Lizza, Ryan, "State of Deception: Why won't the President rein in the intelligence community?", *The New Yorker*, 16 Dec 2013. http://www.newyorker.com/reporting/2013/12/16/131216fa_fact_lizza

[854] Rule, James B., *Privacy in Peril*, Oxford University Press, 2007, pp. 64-65.

[855] The Directive may, however, be in trouble. The EU Court of Justice issued a press release in December 2013 stating that the Advocate General finds the Data Retention Directive to be incompatible with the Charter of Fundamental Rights and constitutes a serious interference with the fundamental right of citizens to privacy. Court of Justice of the European Union, Press Release No 157/13, Luxembourg, 12 Dec 2013. http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157en.pdf

[856] Rule, op. cit., 2007, p. 84.

[857] Coleman, Roy, and Michael McCahill, *Surveillance & Crime*, Sage, London, 2011, pp. 4-5.

[858] Ibid.

4.3 TOMORROW'S SURVEILLANCE SOCIETY

With the advent of the Internet of Things or ambient intelligence, when every manufactured product could be chipped and could become a node in a mesh network of sensors and actuators ("smart dust", as dubbed), the surveillance society of the near future will become even more insidious than it is today. When every product, every device held, used or owned by the individual spins off new information about what individuals are doing, the ability to track and monitor individuals will reach a whole new level of intensity and pervasiveness.

We can also imagine a future where individuals choose to be "enhanced" through the use of certain pharmaceuticals and implants. Governments and industry will be able to monitor these people more easily. There may be incentives to enhance people or enhancements may be reserved only to certain groups such as the military and rich people.[859]

Significant work is taking place in mind-reading techniques, not only for spotting terrorists, but also for playing games or assisting the disabled. The privacy of the mind, of our thoughts and feelings, is the "final frontier" to be conquered, but surveillance of even this frontier can no longer be regarded as the stuff of science fiction.[860]

People will be well and truly mapped. Government authorities and corporation may have vast stores of people's DNA and other biometrics, enabling instant identification.

There is a hint in the Dave Eggers' novel *The Circle* that there might be two societies. Mercer, an ex-boyfriend of the heroine Mae, writes her a letter in which he says,

> If things continue this way, there will be two societies – or at least I hope there will be two – the one you're helping create, and an alternate to it. You and your ilk will live, willingly, joyfully, under constant surveillance, watching each other always… I await the day when some vocal minority finally rises up to say it's gone too far, and that this tool, which is far more insidious than any human invention that's come before it, must be checked, regulated, turned back, and that, most of all, we need options for opting out. We are living in a tyrannical state now.[861]

An alternative, less surveillance-dominated future can also be envisaged. One might foresee that the Snowden revelations generate a sufficient amount of revulsion and resistance among the public that political and corporate leaders are obliged to greatly curtail the surveillance they conduct, that mass surveillance systems are subject to stringent surveillance impact assessments, that where political leaders stand with regard to surveillance rises high on the

---

[859] Wright, David, et al., "Ethical dilemma scenarios and emerging technologies", *Technological Forecasting and Social Change*, Vol. 81, 2014 [forthcoming].
http://www.sciencedirect.com/science/journal/aip/00401625

[860] There have been numerous reports about developments in mind-reading. See, for example, Boffey, Philip M., "The Next Frontier Is Inside Your Brain", Editorial, *The New York Times*, 23 Feb 2013. http://www.nytimes.com/2013/02/24/opinion/sunday/the-next-frontier-is-in-your-brain.html?_r=0. See also Thomson, Iain, "IBM: 'Your PC will read your mind by 2016'", *The Register*, 20 Dec 2011.
http://www.theregister.co.uk/2011/12/20/ibm_five_future_technology; *The Economist*, "The all-telling eye -- We know what you're thinking", 22 Oct 2011. http://www.economist.com/node/21533362; Gardner, Amanda, "Scientists Use Computer to 'Read' Human Thoughts", *US News & Business Report*, 7 Apr 2011. http://health.usnews.com/health-news/family-health/brain-and-behavior/articles/2011/04/07/scientists-use-computer-to-read-human-thoughts

[861] Eggers, Dave, *The Circle*, Hamish Hamilton, London, 2013, p. 367.

electoral agenda, that surveillance becomes something dirty, distasteful and morally corrupt, akin to paedophilia; or not.[862]

Various surveillance experts have contemplated what a future surveillance society will be like. Here are two examples:

Mark Andrejevic provides a glimpse into future surveillance. He identifies three surveillance strategies, i.e., predictive analytics, sentiment analysis and controlled experimentation. Predictive analytics relies upon mining behavioural patterns, demographic information, and any other relevant or available data in order to predict future actions. The goal of sentiment analysis is to take the emotional pulse of the Internet as a whole via Twitter feeds, blogs, social networking sites, online forums, bulletin boards and chat rooms. Marketers use controlled experimentation in interactive environments to subject consumers to an ongoing series of randomised, controlled experiments in order to generate actionable intelligence, to see what works and what doesn't and immediately change their corporate strategy as necessary.[863] Organisations are already exploring these applications; hence, they provide a good signpost into what the emerging future will look like, when such applications come into widespread use and help to manipulate the population.

James Rule asks what further changes in surveillance we can expect in coming years and then contemplates "some uncomfortable futures" such as the state knowing where everyone is at all times, a total population monitoring situation which today's cell phone technology already makes feasible. He envisages a future without cash, one in which all accounts and transactions are computerised and tracked by state agencies. He also envisages a future with "a comprehensive private-sector system for monitoring people's lives as consumers… The system required to accomplish all this would combine the strengths of today's direct-marketing databases with those of insurance and credit reporting systems. It would monitor not only people's total financial situations – accounts, assets, and obligations – but also the timing and content of every consumer transaction."[864] Rule's envisaged futures are a bit more distant, but one cannot help but regard them as perfectly feasible.

Oscar Gandy, David Lyon and others have attempted to steer the conceptualisation of a surveillance society away from simply infringements of our privacy towards the invidious effects of "social sorting". Perhaps the Snowden revelations will help to correct the swing away from privacy. While the "social sorting" of companies, especially the corporate oligarchs, such as Google and Facebook, and government departments intent on uncovering instances of benefits fraud (the low hanging fruit of criminal activity as distinct from corporate malfeasance of bankers and arms producers) is invidious, to be deplored and regulated, the mass surveillance of the intelligence agencies with no meaningful oversight is even more worrying and destructive to democracy. No less worrying, but getting significantly less attention in the media, are the practices of companies such as Nestlé, Shell and McDonald's which use covert methods to gather intelligence on activist groups, counter criticism of their strategies and practices, and evade accountability. "Corporate intelligence gathering has shifted from being reactive to proactive, with important implications for

[862] Freedland, Jonathan, "Why Surveillance Doesn't Faze Britain", *The New York Times*, 8 Nov 2013. http://www.nytimes.com/2013/11/09/opinion/why-do-brits-accept-surveillance.html?_r=0. Freedland is a columnist for *The Guardian*.
[863] Andrejevic, Mark, "Ubiquitous surveillance", in Kirstie Ball, Kevin D. Haggerty and David Lyon (eds.), R*outledge Handbook of Surveillance Studies*, Routledge, Abingdon, 2012, pp. 91-98 [pp. 95-96].
[864] Rule, op. cit., pp. 175-178.

democracy itself," according to research conducted by the Institute for Policy Research at the University of Bath.[865]

The future surveillance society is likely to be marked by more control, more manipulation of citizens and consumers, more asymmetries of power between our corporate and political leaders on the one hand and the bulk of society, on the other. While the future may not be a totalitarian society, it may nevertheless by a tyranny of the minority who control the levers of surveillance, a tyranny with the façade of democracy, no more real than the two-dimensional shop fronts of an old Hollywood western.

4.4 HOW SURVEILLANCE CAN BE USED TO PROTECT SOCIETY

As many surveillance experts insist, one cannot simply paint all surveillance in black and white terms, i.e., where all surveillance is harmful, negative, invidious. Some surveillance applications are beneficial to society and they plus still other applications are either reasonably well accepted by a society or, at least, do not stir much active opposition.

Of course, the perception of benefits depends on who is doing the perceiving. Google, Facebook and other search engines and social networks may view their surveillance activities as essential to their growth and might argue that their growth is good for the overall economy. Similarly, the intelligence agencies such as the NSA and GCHQ will argue that their surveillance activities are aimed at protecting society from terrorists and other criminals. Both groups will be correct in their assertions, but the benefits they gain and confer are not unalloyed. They come with a cost, as discussed in the next section.

From the public's point of view, surveillance can be used to protect society against crime and terrorism in various ways. CCTV cameras helped to identify the terrorists who wreaked havoc in London in 2005 and the Boston Bombers in 2013, although some have argued that surveillance cameras were not so instrumental in apprehending the latter as has been claimed and their role, such as it was, would not justify the installation of more surveillance cameras. Washington University Law professor Neil Richards has argued that there is no evidence to support the proposition that more surveillance cameras would have made Boston safer, that Boston already has a lot of such cameras and, even so, they did not deter the terrorists.[866]

CCTV on transport can help identify muggers. On London buses, video screens show constantly changing real-time videos of all the passengers, which may act as a deterrent to those who might otherwise hassle or mug other passengers. Supermarkets, department stores, and many small shops now have CCTV cameras, partly to help curtail shoplifting, but also apprehend armed robbers who plunder cash registers.

Schools use surveillance systems too. Some have installed biometric devices to read fingerprints and determine who is or isn't in the school and for confirming purchases at lunch. Employers also use such systems, for access control, not only for entry to buildings but to

[865] Institute for Policy Research, "Corporate and police spying on activists undermines democracy", University of Bath, 2012. http://www.bath.ac.uk/ipr/pdf/policy-briefs/corporate-and-police-spying-on-activists.pdf. This policy brief notes that co-operation between the government and corporate intelligence in such secret operations is a seriously neglected field of research.
[866] Richards, Neil M., "Surveillance state no answer to terror", *CNN*, 23 Apr 2013. http://edition.cnn.com/2013/04/23/opinion/richards-surveillance-state

sensitive areas within the buildings, e.g., to restricted areas where high value bids are evaluated.

Airports are major hubs for various surveillance technologies, including body scanners. Although some passengers are inconvenienced by the security checks, by far the vast majority of passengers accept being surveilled comprehensively before embarking on an airplane.

DNA databases are controversial, but there is no denying that they have helped to catch criminals or confirm that some suspects are innocent.[867] The 2008 S and Marper decision by the European Court of Human Rights said the UK government's retaining the DNA of those not convicted was an intrusion upon privacy and that the relevant DNA samples were to be removed from the database, a decision with which the UK government has been slow to comply.[868]

Security agencies and their supporters emphasise the need for surveillance technologies. The head of the UK's MI5 security service Andrew Parker argued in October 2013 that the surveillance measures used by GCHQ, the government's spy agency, were needed "at a time when the UK is facing its gravest terror threat, including from 'several thousand' Islamist extremists who are living here [in the UK] and want to attack the country".[869] Parker added that "With the spread of an al-Qaeda threat to more and more countries, the continued danger of Irish terrorism, the emergence of the lone wolf fanatic and advances in technology and cyber warfare, MI5 is now 'tackling threats on more fronts than ever before".

Such remarks sow fear. Some politicians and intelligence agencies sow fear to justify the increasingly large expenditures on surveillance. Peter Ludlow, a professor of philosophy at Northwestern University, wrote in *The New York Times* that "Even democracies founded in the principles of liberty and the common good often take the path of more authoritarian states. They don't work to minimize fear, but use it to exert control over the populace and serve the government's principal aim: consolidating power."[870] Ludlow argues that the fear of terrorists is the pretext for establishing the surveillance state. He suggests that "the more immediate danger to our democratic society comes from those who lurk in the halls of power in Washington and other national capitols and manipulate our fears to their own ends. What are these ends? They are typically the protection of moneyed interests."[871]

More prosaically than the use of surveillance to detect al-Qaeda, law enforcement authorities use surveillance technologies, such as drones, to surveil crowds at a football match, hunting for trouble-makers and yobs.

---

[867] Coleman and McCahill note that between 2004 and 2009, the UK DNA Database more than doubled in size, yet the proportion of recorded crimes detected using DNA remained steady at 0.36 per cent. Coleman and McCahill, op. cit., 2011, p. 171.

[868] Travis, Alan, "Ministers keep innocent on DNA database", *The Guardian*, 7 May 2009. http://www.guardian.co.uk/politics/2009/may/07/dna-database-government-retention

[869] Whitehead, Tom, "GCHQ leaks have 'gifted' terrorists ability to attack 'at will', warns spy chief", *The Telegraph*, 8 Oct 2013. http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10365026/GCHQ-leaks-have-gifted-terrorists-ability-to-attack-at-will-warns-spy-chief.html

[870] Ludlow, Peter, "Fifty States of Fear", *The New York Times*, 19 Jan 2014. http://opinionator.blogs.nytimes.com/2014/01/19/fifty-states-of-fear/?_php=true&_type=blogs&_r=0

[871] Ibid.

Surveillance projects such as Google Flu Trends and Flu Near You[872], a crowd-sourced flu tool, offer social benefits in identifying and tracking flu trends so that the public is better informed about the location and severity of outbreaks.[873] In Australia, researchers say that surveillance and mapping of Internet searches and social media topics could help detect epidemics quicker than traditional methods that rely on patients seeking treatment from a physician who in turn alerts authorities of infectious disease cases.[874]

Surveillance can be used to help protect society against fraudulent claims of social service benefits, but as already mentioned surveillance has had no noticeable impact on preventing or apprehending corporate fraudsters. A former UK Director of Public Prosecutions said fraudulent bankers represent more of a risk to the public than muggers or terrorists.[875]

Surveillance has benefits for national security, criminal justice, emergency response, public administration and medical care. "But there is a line between surveillance that is essential for the public good and invasive total-information awareness technologies, and that line is easy to cross if unattended. This leaves us with the question of how to protect society from the gradual acceptance and institutionalization of total-information awareness technologies."[876]

4.5 How surveillance can undermine the freedoms and values it aims to protect

Surveillance – whatever its benefits in coping with the kinds of threat mentioned above – may itself pose a threat to individuals, societies, and communities because of its ubiquity, intensity, and use of personally identifiable information. These qualities of surveillance may erode privacy and a host of freedoms, rights and values (such as those listed below) that it is designed to protect, including democracy itself. This creates a negative perception of surveillance. As James Rule has observed, "Surveillance systems created for the most banal or even benevolent purposes can readily serve as instruments for oppression."[877]

In this section, we provide examples of how surveillance can threaten or erode these freedoms and values.

Privacy and data protection

Lee Bygrave, Associate Professor in the Faculty of Law, University of Oslo, is of the view that "surveillance, by its very definition, involves a reduction of privacy." However, he has argued that it is more difficult to gauge the effect of surveillance on perceptions of freedom, because people can "go around thinking they are free even though they are really in some sort

[872] https://flunearyou.org/
[873] Moore, Elizabeth Armstrong, "Latest flu-related tech is largely about the greater good, not you", *CNET News*, 25 Jan 2014. http://news.cnet.com/8301-11386_3-57617783-76/latest-flu-related-tech-is-largely-about-the-greater-good-not-you/
[874] ABC News Online, "Queensland researchers begin development of system to detect disease outbreaks online", 3 Feb 2014. http://au.news.yahoo.com/a/21243639/queensland-researchers-begin-development-of-system-to-detect-disease-outbreaks-online/
[875] The Times, "Rogue bankers 'more a threat than terrorists'", 23 Feb 2009. Cited by Coleman, Roy, and Michael McCahill, *Surveillance and Crime*, Sage, London, 2011, p. 180.
[876] Citron, Danielle Keats, and David Gray, "Addressing the harm of total surveillance: A reply to Professor Neil Richards", *Harvard Law Review Forum*, Vol. 26, pp 262-274 [p. 272].
[877] Rule, James B., *Privacy in Peril*, Oxford University Press, 2007, p. 42.

of aquarium." [878] This is quite a good metaphor for describing the situation in which modern surveillance societies present themselves.

Trust and transparency

The 2008 House of Commons on surveillance noted that "Loss of privacy through excessive surveillance erodes trust between the individual and the Government".[879] The earlier SSN report prepared for the UK ICO said something similar, i.e.,

> surveillance processes and practices bespeak a world where we know we're not really trusted. Surveillance fosters suspicion. The employer who installs keystroke monitors at workstations, or GPS devices in service vehicles is saying that they do not trust their employees. The welfare benefits administrator who seeks evidence of double-dipping or solicits tip-offs on a possible 'spouse-in-the-house' is saying they do not trust their clients. And when parents start to use webcams and GPS systems to check on their teenagers' activities, they are saying they don't trust them either. Some of this, you object, may seem like simple prudence. But how far can this go? Social relationships depend on trust and permitting ourselves to undermine it in this way seems like slow social suicide.[880]

In short, surveillance erodes transparency and trust, which in turn erodes societal cohesion and democracy itself. If we (the public) don't trust our "democracies", then that lack of trust unravels the fabric of democracy itself.

Dignity

For many people, having to submit to body scanners, especially those that are the visual equivalent of a strip search, is an affront to our dignity. Similarly, the monitoring of our communications by intelligence agencies is an affront to our dignity. It undermines our sense of self-worth.

Autonomy

Surveillance systems may curtail our range of choices. David Lyon and others regard social sorting as a key feature of modern surveillance systems. Social sorting "pigeon holes" us: it puts us in a certain group which, almost inevitably, will have fewer opportunities – even as consumers, we may not have the full range of choices that others might have. The fewer the choices we have, the more our autonomy is constrained.

Freedom of movement

Today's smart phones with their myriad applications might seem "pretty cool", but the reality is that they are tracking devices. Some of the tracking is relatively benign and even socially useful, for safety reasons, and some of the tracking is convenient, such as new social media services, such as FourSquare that alert us to the nearby presence of shops or people of like mind (e.g., friends or dating prospects). Some of the tracking, however, is a constant, ongoing

[878] House of Lords Select Committee on the Constitution, House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, Volume I: Report, 2nd Report of Session 2008–09, The Stationery Office, London, 6 Feb 2009, p. 14.
[879] House of Commons Home Affairs Committee, *A Surveillance Society?*, Fifth Report of Session 2007–08, Volume I, The Stationery Office, London, 8 June 2008, p. 5.
[880] SSN, op. cit., 2006, p. 3.

threat to our privacy. Some of the tracking takes place in the physical world and some in cyberspace. There are trade-offs. Is the tracking of every car on every highway and every street acceptable, even if reduces the number of fatalities? Is tracking everyone's movements on the Internet justified, even if it helps to catch a few terrorists?

Freedom of thought and expression

Our minds are the last frontier of privacy. Surveillance technologies might be able to track us, watch what we are doing, everywhere and all the time, in physical and cyberspace, might be able to record everything we do, but they have yet to burrow inside our heads. What goes on within our cranium, so far, has been off-limits. But many scientists and technology developers are putting tentacles even there; and in many cases, law enforcement authorities, intelligence agencies, companies and other wrong-doers don't even need such technologies. Much about our inner sanctum can be deduced from our behaviour, our actions, from what we buy, from the people with whom we associate, from what we say and write, from the images we post online. As in *1984*, Big Brother has a chilling effect. People (or at least some people) become more circumspect about what they say, write and do. This chilling effect curtails our creativity, our freedom of thought and expression and our sense of that freedom. Awareness of ubiquitous surveillance can stifle the vibrancy and creativity of society, as Bart Jacobs observes: "The greater the uncertainty about what precisely is stored in your profile and triggers a reaction, the greater the fear and tendency towards conformism. Conformism is however not what has made western societies excel (industrially or scientifically, for instance)."[881]

Freedom of association and right to lawful protest

The chilling effect extends to freedom of association. The presence of surveillance cameras may have a chilling effect on some people who will not participate in a demonstration if they know they are likely to be recorded and identified. Some people may not go to a football match if they know their facial images might be recorded. Some people may not associate with other people if they know they are going to be watched and recorded. Whistle-blowers might think twice about contacting journalists if they know they are going to be recorded.

Freedom of information

Secrets laws and orders are inimical to democracy. Surveillance societies, such as the US and UK, have secret laws and orders. Transparency and freedom of information are essential prerequisites for holding officials (governmental and corporate) accountable for their actions. If officials can hide behind secret laws and orders, they cannot be held accountable.

Perpetuation of social inequalities

Some people, some neighbourhoods, some modes of transport, some places are more surveilled than others. Coleman and McCahill point out that surveillance is "uneven both in its reach into society and in its consequences".[882]

Torin Monahan argues that "contemporary surveillance systems are antithetical to democratic ideals both in their design and application. They individualize, objectify, and control people –

[881] Jacobs, op. cit., p. 28.
[882] Coleman, Roy, and Michael McCahill, *Surveillance & Crime*, Sage, London, 2011, p. 8.

often through their use of data – in ways that perpetuate social inequalities… Especially by shutting down avenues for meaningful participation (or representation) in design processes that affect most people's lives and by aggravating social inequalities, surveillance systems threaten democracy."[883]

Social integration and societal solidarity

Social sorting hinders, indeed is invidious to, social integration and societal solidarity. Surveillance betrays a lack of trust. If employees are surveilled, it may mean that employers do not trust them, that they may think employees will be surfing the Internet, playing games or watching porn on company time. If people know that some neighbourhoods are surveilled while minimal or no effective oversight of corporate crime takes place, it increases the distance between the privileged and welfare recipients.

The rule of law, due process and the presumption of innocence

Pervasive, relentless surveillance assumes we are all suspects. Mass surveillance, nominally used to prevent crime and terrorism, may be used to link dots where none exist. Cardinal Richelieu reputedly once said, "Qu'on me donne six lignes écrites de la main du plus honnête homme, j'y trouverai de quoi le faire pendre."[884] In similar fashion, surveillance can be used to condemn even the innocent. The pre-crime unit in Spielberg's *Minority Report* is a warning that surveillance can be used to apprehend people who have yet to (or may never commit) a crime. Ben Hayes also worries about the trend from "reactive to proactive security. Governments and state agencies no longer just respond to crimes, instead they try to pre-empt them by identifying and neutralizing risks before threats to security can be realized."[885]

4.6 WHOSE RESILIENCE?

Resilience can apply to both systems and people. Engineers regard a telecom system as resilient if it can withstand a failure somewhere in the network and still manage to deliver traffic to its destination. Similarly, an infrastructure can be regarded as resilient if it can successfully withstand attacks. However, in the context of resilience in a surveillance society, our focus is on people.

Resilience, furthermore, is a scalable quality, i.e., it can apply to individuals, households, communities, organisations and societies. It is important to clarify whose resilience we refer to in a discussion of resilience in surveillance societies. Kolliarakis contends that the crucial question of "resilience of whom, against what" is often side-stepped.[886]

Political and corporate leaders who wield power in a surveillance society may view surveillance systems as an important instrument of *their* power, of maintaining *their* power. Hence, their resilience, their avoidance of the shocks or stresses that might come with attempts by the surveilled to curtail their power, may depend on their ability and capacity to surveil the population as deeply, as intensely and, preferably, as secretly as possible. When

[883] Monahan, Torin, "Surveillance policies and practices of democratic governance", in Kevin D. Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, Abingdon, 2010.
[884] "If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him." Quoted in J.K. Hoyt, *The Cyclopedia of Practical Quotations*, Funk & Wagnalls, 1896, p. 763.
[885] Hayes, op. cit., p. 169.
[886] Kolliarakis, op. cit, 2013, p. 8.

the extent of their surveillance is discovered, their resilience lies in their power to resist any curtailment in the extent of their surveillance practices. Google, Facebook and other corporate powers as well as the NSA and GCHQ have so far successfully resisted attempts to cut back in any significant way their surveillance practices.

The resilience of law enforcement authorities, intelligence agencies, industry and others may also depend on their inventiveness in devising new surveillance technologies and systems and, again, to conduct their surveillance as secretly as possible, unknown to the target(s).

Advocacy groups, the media, academia and some other stakeholders, including the public, may view resilience as a way of attempting to minimise the surveillant's power over them.

Authoritarian regimes can be just as resilient as democracies, as Andrew J. Nathan has demonstrated in his analysis of the resilience of China's leadership. "Regime theory holds that authoritarian systems are inherently fragile because of weak legitimacy, overreliance on coercion, overcentralization of decision making, and the predominance of personal power over institutional norms. This particular authoritarian system, however, has proven resilient."[887] Concluding his analysis, Nathan suggests the disturbing possibility that "authoritarianism is a viable regime form even under conditions of advanced modernization and integration with the global economy".[888] If surveillance is antithetical to democracy, then one cannot discount the possibility that it will be just as difficult, improbable or perhaps impossible to transform a surveillance society, as advanced as it already is, as it will be for the Chinese population to transform China into a democracy – to transform a surveillance society into a more democratic regime where the people (the demos) are able to control the surveillance systems that currently manipulate their behaviour, limit their choices and search out deviants who might be criminals or terrorists or simply political activists aiming to restore power to the people. From a theoretical perspective, this prompts the question whether complex societies can be governed in a democratic way or whether they can be governed at all. In political theory the classical model of government has been replaced with the concept of (multi-level) governance. Whereas government entertains the idea of a central institutionalised centre of power drawing its legitimacy from democratic elections and executing collectively binding decisions, governance operates with many dispersed centres of power, interlinked but autonomous, cooperating and negotiating solutions for partial problems under different regulatory regimes.

With regard to resilience the interesting question is: to what extent individuals who are affected by decisions taken somewhere in the world wide web of nodal multi-level governance can influence these decisions in a meaningful way. Surveillance would be a paradigmatic test case to tackle this problem: is it conceivable for citizens to be involved in decisions about the collection, processing and use of personal data, when these decisions are taken at some remote place by a group of people beyond the reach of democratic control? Can the (detrimental) effects of such a surveillance regime be discussed, negotiated, prevented by means of democratic action that qualifies as "resilience"? These are complex questions and there are no easy answers available.

[887] Nathan, Andrew J., "Authoritarian Resilience", *Journal of Democracy*, Vol. 14, No. 1, January 2003, pp. 6-17 [p.6].
[888] Ibid., p. 16.

4.7 IS RESISTANCE A RESILIENCE STRATEGY OR ARE RESILIENCE AND RESISTANCE DIFFERENT THINGS?

Preparedness (which is anticipatory) is nominally a form of resilience. In the UK, the Civil Contingencies Act requires emergency responders to hold regular exercises to prepare for future potential emergencies. Uncertainty becomes an opportunity to speculate not just about the future, but about a range of possible futures. However, according to Claudia Aradau, preparedness exercises do not imagine an overturning of the present social order: "Activating subjects to anticipate the future through preparedness exercises is not to inhabit a future where failings of the present would be overcome."[889] Transferring this thinking to resilience in a surveillance society suggests that resilience in the sense of preparedness is limited and limiting – i.e., it becomes a way of responding to a future where surveillance remains, rather than a future without surveillance. Or, if surveillance is to remain a feature of modern life, as numerous writers point out, then control or oversight of surveillance should shift from politicians, corporate warlords and intelligence agencies to regulators empowered by stakeholders representing the public.

Aradau's *Radical Philosophy* colleague Mark Neocleous takes her notion a step further, i.e., by contending that "resilience is by definition *against resistance*. Resilience wants acquiescence, not resistance. Not a passive acquiescence, for sure, in fact quite the opposite. But it does demand that we use our actions to accommodate ourselves to capital and the state, and the secure future of both, rather than to resist them."[890] Should we regard resistance as a form of resilience or should we regard them as diametrically opposed to each other? Is resilience, as Neocleous implies, an acceptance of the world order?

Béné et al. regard resistance as an element of resilience. They propose three components of a resilience framework: absorptive, adaptive and transformative. They suggest that these different responses can be linked (at least conceptually) to various intensities of shock or change. The lower the intensity of the initial shock, the more likely the household (or individual, or community or system) will be able to *resist* it effectively, i.e., to absorb its impacts without consequences for its function, status or state.

> When the absorptive capacity is exceeded, the individual will then exercise their adaptive resilience (Cutter et al. 2008). This adaptive resilience refers to the various adjustments (incremental changes) that people undergo in order to continue functioning without major qualitative changes in function or structural identity… if the change required is so large that it overwhelms the adaptive capacity of the household, community or (eco)system, transformation will have to happen. In that case, changes are not incremental any longer. Instead they are transformative, resulting in alterations in the individual or community's primary structure and function… the main challenges associated with transformation are not of a technical or technological nature only. Instead, as pointed out by O'Brien (2011), these shifts may include a combination of technological innovations, institutional reforms, behavioural shifts and cultural changes; they often involve the questioning of values, the challenging of assumptions, and the capacity to closely examine fixed beliefs, identities and stereotypes. In other words, they challenge status quo.[891]

---

[889] Aradau, Claudia, "The myth of preparedness", *Radical Philosophy*, RP 161, May/Jun 2010.
[890] Neocleous, Mark, "Resisting resilience", *Radical Philosophy*, RP 178, March/April 2013.
[891] Béné, Christophe, Rachel Godfrey Wood, Andrew Newsham and Mark Davies, "Resilience: New Utopia or New Tyranny? Reflections about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes", IDS Working Paper, Vol. 2012, No. 405, CSP Working Paper Number 006, Institute of Development Studies, September 2012, pp. 21-22.

Pat Longstaff, on the other hand, distinguishes between resistance (keeping a danger away) and resilience (bouncing back if the bad thing happens).[892] However, resistance in a surveillance society is not so much about keeping a danger away (although that could be part of it), as undermining it (e.g., putting a bag over a CCTV camera), deflecting it (e.g. declining a loyalty card) or overcoming it (e.g. public rejection of an ID card system).

4.8 RESISTANCE

As noted before, resilience commonly means being able to bounce back to a previous state or to recover from an adverse event. However, resistance does not mean "bouncing back" to a previous state or recovering from an adverse event; it means resisting the oppression of an existing state, of not accepting the status quo, of finding inner strength in resisting an established order. Hence, resilience and resistance are different things, but, at the same time, one can see an overlap, especially to the extent that resistance can be regarded as a strategy of resilience.

Coleman and McCahill define resistance to surveillance as follows:

> Any active behaviour by individuals or interest groups that opposes the collection and processing of personal data, either through the micro-practices of everyday resistance to defeat a given application, or through political challenges to defeat a given application, or through political challenges to wider power relations which contest the surveillance regime per se.[893]

Citing Hollander and Einwohner, Coleman and McCahill note two elements common to the use of the concept: First, resistance usually involves some active behaviour (verbal, cognitive or physical) and second, resistance nearly always involves a sense of opposition or challenge. However, these elements raise two important questions: Who is doing the resisting and who or what is being resisted. They note also that resistance can involve individuals acting alone or groups acting in concert.[894]

Resistance has different meanings or may take different forms in different contexts or situations. Resistance which involves destroying property (e.g., third-party fingerprint scanners used at schools to admit students) is different from legal challenges by advocacy organisations to overturn proposals for new surveillance legislation. Resistance can take the form of complaints, boycotts, demonstrations, civil disobedience, vigilante groups, physical attacks and cyberattacks aimed at changing the balance of power between the surveillants and the surveilled. However, it should be noted that increasing surveillance undermines the socio-cultural and cultural political infrastructure for such activities.

Other relevant terms are mitigation and dissent. One can envisage mitigating the worst effects of a surveillance technology or system through using a surveillance impact assessment in which stakeholders are consulted and engaged. In the case of dissent, an advocacy organisation might try to organise public opposition to a new measure, as was the case with regard to the proposed introduction of an ID scheme in the UK. While dissent could be regarded as an act of resistance, mitigation could be regarded as a form of resilience.

---

[892] Longstaff, P.H., *Security, Resilience, and Communication In Unpredictable Environments Such as Terrorism, Natural Disasters and Complex Technology*, Center for Information Policy Research, Harvard University, Cambridge MA, Nov 2005, p. 4.
[893] Coleman, Roy, and Michael McCahill, Surveillance & Crime, Sage, London, 2011, p. 147.
[894] Ibid., p. 145.

No handbook on resilience in surveillance societies would be complete without a reference to Gary T. Marx's catalogue of resistance possibilities. In his 2003 paper, "A tack in the shoe", he lists 11 types of response to privacy-invading surveillance: discovery moves, avoidance moves, piggybacking moves, switching moves, distorting moves, blocking moves, masking (identification) moves, breaking moves, refusal moves, cooperative moves, and counter-surveillance moves. [895]

Even if resistance is possible, some people may not resist surveillance (even if the surveillance practice is known), as Marx notes:

> a lack of resistance to intrusive surveillance may mask as acceptance because of a fear of being sanctioned or losing one's job, position, or privilege, or as a necessary condition for something desired such as employment, credit, apartment or car rental, air travel, or government benefits. There may also be fatalism and resignation for the individual, believing it is impossible to resist… [as reflected in statements such as] "I have nothing to hide," "It's for my own good," "I support the goals," "I'm getting paid," "It's just the way they do things here," "They have to do it to ... [stay competitive, obtain insurance, stop crime, avoid risks]".[896]

But Marx does not despair of those resigned to surveillance. On the contrary, he is optimistic: "Humans are wonderfully inventive at finding ways to beat control systems and to avoid observation. Most surveillance systems have inherent contradictions, ambiguities, gaps, blind spots and limitations, whether structural or cultural, and, if they do not, they are likely to be connected to systems that do." [897] He also says that people will break rules if they regard an organisation or its surveillance procedures as unacceptable or illegitimate, untrustworthy or invalid, demeaning, unnecessary, or irrelevant.[898]

It is also important to note who is doing the resisting and why they are resisting. In some (most) cases, the surveillance practices, technologies and systems will be truly and unduly intrusive. In such cases, there may be legitimate reasons for resisting surveillance. In other cases, however, criminals, terrorists or welfare cheats may seek to evade surveillance. But evading surveillance is not exactly the same as resisting it. The criminal might smash a CCTV camera (resistance) or he might wear a baseball cap and dark glasses to avoid recognition (evasion).

4.9 HOW TO INTERPRET RESILIENCE IN THE CONTEXT OF A SURVEILLANCE SOCIETY

Resilience originally, typically, meant a return to a previous state, a recovering from a shock, a bouncing back after a crisis. However, the definition of resilience has evolved, and now can be used to signify anticipatory activity as well. Further, what is necessary to resist a shock may be quite different from what is needed to adapt to it. Similarly, in a surveillance society, there is clearly a difference between resisting surveillance and adapting to it.

Resilience in the context of surveillance is different from resilience in the instance of the capacity of an infrastructure or of a community disrupted by an earthquake or a tsunami or a financial calamity. Although it may come as a shock or a revelation to some people when they

[895] Marx, Gary T., "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 369-390.
[896] Ibid., p. 370.
[897] Marx, op. cit., 2003, p. 372.
[898] Marx, op. cit., 2003, p. 372-373.

realise how extensive and pervasive surveillance has become, much of the surveillance today can be regarded as an ongoing stress on society, rather than a shock. Hence, resilience in a surveillance society has more to do with coping than with only recovering or bouncing back.

Those studying resilience of communities in developing countries are right to raise questions about the vulnerabilities and risks faced by such communities, and resilience in this sense is relevant to a surveillance society too. It is appropriate for academics, advocacy organisations and the news media to ask questions about the vulnerabilities of our society, of the frailty of our democratic traditions in the face of increasing surveillance. It is not enough to simply focus on the infringements of surveillance to privacy. We also need to question how the surveillance systems came to be: who authorised them and under what circumstances (were surveillance systems introduced as a result of industry lobbying efforts)? To what extent were stakeholders, including the public, consulted and engaged in the decision-making process? Are such systems actually necessary? Are there alternatives to the introduction of a surveillance system?

Ben Hayes argues that the "surveillance-industrial complex" has a corrosive effect on political culture, democratic governance and social control.[899] He states the surveillance-industrial complex extends throughout the "surveillance society", from the workplace to the World Wide Web. According to Hayes "the global reach of many security and surveillance contractors raises complex jurisdictional problem in terms of holding them and their employers to account".[900] He argues that the security industry has heavily influenced the research agenda in the EU (as in the US) and that the industry profits from the research spend of the European Commission, not only directly in terms of contracts, but also in terms of policy. "The roll-out of high-tech surveillance systems implicitly threatens privacy and civil liberties, yet the democratic structures we rely on to protect those rights and freedoms appear to have been marginalized by a creeping technological determinism."[901]

To the extent that one could equate resilience with "coping" with surveillance, it would suggest that one is simply "surviving" in a surveillance society or simply reacting to the impacts of surveillance on one's life. Resistance, on the other hand, is more pro-active, less willing to accept the status quo.

In the resilience literature, some authors believe that resistance is an element in resilience strategy, while others believe that resistance and resilience are different things, but a third possibility, one that the present authors prefer, is that, while resistance and resilience are generally different, there is some overlap, so one can depict the situation as follows:

[899] Hayes, Ben, "The surveillance-industrial complex" in Kirstie Ball, Kevin D. Haggerty and David Lyon (eds.), R*outledge Handbook of Surveillance Studies*, Routledge, Abingdon (UK), 2012, pp. 167-175 [p. 167].
[900] Hayes, op. cit., 2012, p. 171.
[901] Hayes, op. cit., 2012, p. 174.

Figure 5 Resilience-resistance overlap

Resilience in the context of telecommunications and information networks is a function of what engineers might regard as an acceptable grade of service. In a surveillance society, we can ask how much surveillance is society willing to accept? At what point does excessive surveillance create a dysfunctional society and who has the power to determine what dysfunctionality means? Do citizens have a choice regarding whether the surveillance measure is to be introduced or not? If citizens can anticipate new surveillance measures, can they dissent? Can they exercise any influence to avoid the introduction of new surveillance measures, by either the government or companies?

Resilience and resistance can both be analysed or promoted at the level of the citizen as well as groups or society as a whole.

It is apparent that there are different resilience strategies. Coping is one, resistance is another. Surrender might be a third, i.e., in order to survive, one surrenders. In a surveillance society, surrender would mean that one accepts the ubiquitous presence and inevitability of surveillance. One can no longer contemplate resistance. Privacy is lost, both for the individual and for society. If one accepts that privacy is a cornerstone of democracy, the loss of privacy also means a loss of democracy. Democracy is supplanted by a new and insidious authoritarianism that might preach its adherence to democratic values, that might preach the necessity of surveillance in order to counter threats to democratic order from terrorists and criminals, but the reality is that this is a hollowed-out democracy, a mere semblance of democracy that disguises the power and omnipotence of an oligopoly of surveillants. Thus, one might see resilience as on a continuum somewhere between surrender and civil disobedience.

Resistance can be active in the sense of destroying or blacking out CCTV cameras or using onion routing when using the Internet or other such strategies. It might also mean re-asserting citizen control of surveillance, e.g., by demanding better oversight of surveillance practices and systems, by greater transparency of who are the surveillants, who are they surveilling, why they are surveilling either individuals or groups within society or the whole of society, how they are being funded, what reporting mechanisms are in place and so on. Resistance could also mean the power to say “No” to an existing or proposed system – to disallow some forms of surveillance.

Resistance need not be an “all-out” strategy, whereby those resisting surveillance are against all forms of surveillance. Resistance can be total or selective. Selective resistance means that

one might oppose some forms of surveillance (mass surveillance versus targeted surveillance) but not all.

If citizens or their elected representatives are able to assert some control over surveillance systems and practices, or if they are truly and successfully able to say "No", this could also be viewed as a form of resilience in the sensing of "bouncing back", i.e., society is able to return to some previous state before a surveillance system or practice materialised – or if it had already materialised, that society is capable of ordering its dismantling. If this is the case, then resilience could be regarded as more than simply coping. Even if one is able to return or "bounce back" to a previous state, the "status quo ante" will almost certainly be elusive to the extent that citizen trust will remain broken or, at best, damaged. Suspicion is likely to remain a feature of both resistance and resilience. A healthy suspicion of existing, prospective and potential surveillance systems will serve as their counter. While trust is an essential ingredient in a functioning democracy, in an advanced surveillance society, suspicion is needed in equal measure.

Crisis management and mitigation might also characterise some forms of resilience. Thus, one displays resilience if one attempts to mitigate the negative effects of surveillance. Similarly, if one regards surveillance as a crisis for democracy, then crisis management can be regarded as a form of resilience.

Resilience and resistance strategies could include transparency and accountability – i.e., those who (wish to) conduct surveillance must provide some degree of transparency with regard to how and where the system is used, who operates the system, what checks and balances exist, public access to gathered data and rectification of errors, etc. Transparency is necessary to ensure effective accountability. Unless transparency exists, it will be impossible to hold someone to account for the surveillance system.

Accountability presupposes de facto and de jure legality. Hence, surveillance systems should be established within the limits of the law, if not by law itself. Further, they must comply with the law. In theory, the law is a form of resilience and/or resistance. The law does not give free reign to operators of surveillance systems to do as they like. The law sets limits on surveillance. At least, that is the theory. In reality, many surveillance systems are created outside the law and certainly don't comply with it. To the extent that the law is not enforced, it encourages other surveillance operators to operate outside the law, to disrespect and ignore the law.

Some could argue (or have argued) that accountability is a kind of Trojan horse – it legitimises a practice. It could be regarded as a tacit acceptance of surveillance. Laws can also act as a kind of Trojan horse – laws may have certain exemptions permitting surveillance where national security or economic well-being are at stake (or *perceived* to be at stake). Such exemptions may lead to serious abuse, as journalists have discovered from the Snowden revelations. Even the strictest of legal regulations in the field of surveillance often have a kind of back door, providing a formal legal basis for extensive and comprehensive surveillance measures under certain circumstances. Typically, legal safeguards lose their limiting force when it can be demonstrated that for reasons of national security or serious threats to public order, intensive surveillance measures have to be taken. Such threat assessments are largely produced by the security and law enforcement agencies who are often the main beneficiaries of extensive surveillance, strengthening their administrative and political powers.

It is possible to resist surveillance, but resistance may not prevent surveillance. But one can be sanguine: for instance, the European Parliament's LIBE committee report on the NSA revelations can be regarded as a form of resistance and prevention.

4.10 SURVEILLANCE AND POWER

Oscar Gandy argued in 1993 that issues of surveillance relate directly to questions of power.[902] Others have made similar observations. David Lyon has pointed out that "power relations are intrinsic to surveillance processes".[903] He adds that "It is not merely that some kinds of surveillance may seem invasive or intrusive, but rather that social relations and social power are organized in part through surveillance strategies."[904] In line with Bart Jacobs view referenced earlier, Lyon comments, "The idea that state power could be augmented by surveillance systems in ways that are at least reminiscent of totalitarianism is quite plausible."[905] However, he adds, "There is much more to contemporary surveillance than totalitarianism or panopticism, significant though these concepts are." [906] He points to the increasing convergence of once discrete systems of surveillance. He also points out that new technologies empower the watched too – "internet blogs, cell-phone cameras and other recent innovations may be used for democratic and even counter-surveillance ends".[907] While this may be true to some extent, the Snowden revelations show that the surveillance capacity of the NSA and GCHQ are far beyond the capacity of a few cell phone cameras to counter.

The "empowered watched" are no match for the surveillance power of the intelligence agencies or big corporations such as Google and Facebook, as Coleman and McCahill argue:

> Despite some evidence of a 'rhizomatic levelling' of surveillance, the ability to conduct surveillance or to establish and legitimate a surveillance regime remains concentrated in the hands of 'dominant' groups. Moreover… there is often an overlapping, or closer 'correspondence of interests', between the surveillant authorities and the 'powerful', evident in the greater tolerance and limited surveillance of the harms, injurious events and criminal activities committed by this group. This situation was contrasted to the surveillance practices targeted at the 'powerless', which resulted in further marginalisation, disorganisation and disruption of their life chances.[908]

There is clearly an asymmetry of power between the individual, groups and society as a whole on the one hand and organisations and state authorities who initiate or implement surveillance measures on the other. Surveillance is an instrument of control, as Torin Monahan remarks:

> At its core, surveillance is about control; it tends to produce conditions of constraint, wherein human and technical action is regulated and limited… such systems are most often characterized by coercion and repression, and offer few avenues for accountability or oversight… Commercial surveillance of people for marketing purposes betrays a similar trend… surveillance practices, share a set of characteristics that are clearly non-democratic.

---

[902] Gandy, Oscar H., *The Panoptic Sort: A Political Economy of Personal Information*, Westview Press, Boulder, CO, 1993.
[903] Lyon, David, "Surveillance, Power, and Everyday Life", in Robin Mansell, Chrisanthi Avgerou, Danny Quah and Roger Silverstone (eds.), *The Oxford Handbook of Information and Communication Technologies*, Oxford University Press, 2009, pp. 449-472.
[904] Ibid.
[905] Lyon, op. cit., 2009.
[906] Lyon, op. cit., 2009.
[907] Lyon, op. cit., 2009.
[908] Coleman, Roy, and Michael McCahill, *Surveillance & Crime*, Sage, London, 2011, p. 147.

> They each open people up to examination and control, while constraining individual autonomy. They each rely upon opacity instead of transparency; most people under surveillance have little knowledge of the inner workings of the systems or their rights as citizens, consumers, or others. Finally, because these systems are closed, they resist opportunities for democratic participation in how they are designed, used, critiqued or regulated.[909]

It is only possible to dislodge control if one has knowledge of the power structures and the instruments of control. However, the public generally does not have knowledge of the "weak" points in power structures. There has been a gap in knowledge between the public ill-informed about the true extent of surveillance in society and the surveillance cognoscenti, but the Snowden revelations have helped to change that. The intense media coverage of the Snowden revelations, especially in the US and Europe, has helped to overcome some of this knowledge gap.

A particularly big gap in knowledge has been the close relationship between political and corporate power, and how each buttresses the other. Robert O'Harrow showed that, in the days immediately after 9/11, some data aggregators offered their services to the US government to engage in some data mining that might show who were or are terrorists.[910] The Bush administration took up such offer and, in doing so, helped to foster a closer alliance of state and corporate power. The Statewatch NeoConOpticon report revealed similar alliances between the security industry and political power, as wielded by the European Commission and the intelligence agencies.

4.11 MEASURES TO INCREASE RESILIENCE IN A SURVEILLANCE SOCIETY

The following sections outlines various measures to increase resilience in a surveillance society. This list is based on the research conducted and is not exhaustive.

4.12 POLITICAL AND REGULATORY MEASURES

The 2008 House of Commons report on surveillance cited earlier advocated "The decision to use surveillance should always involve a publicly-documented process of weighing up the benefits against the risks, including security breaches and the consequences of unnecessary intrusion into individuals' private lives."[911] Today we could term such a process as a surveillance impact assessment. The House of Commons Home Affairs Committee, which carried out the study, made the tepid recommendation that "the Home Office exercise restraint in collecting personal information, and address the question of whether or not surveillance activities represent proportionate responses to threats of varying degrees of severity". In the following pages, we consider some of the measures that should be taken into account in considering the need for surveillance systems, especially mass surveillance systems.

4.12.1 Accountability and oversight

[909] Monahan, Torin, "Surveillance as governance: Social inequality and the pursuit of democratic surveillance", in Kevin D. Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, Abingdon, UK, 2010, pp. 91-110 [p. 91].
[910] O'Harrow, Jr., Robert, *No Place to Hide*, Free Press, New York, 2005.
[911] House of Commons Home Affairs Committee, *A Surveillance Society?*, Fifth Report of Session 2007–08, Volume I, The Stationery Office, London, 8 June 2008, p. 5.

Priscilla Regan argued in 1995 that privacy has not only an individual value, but also a social value and, accordingly, organisations that use such data have to give account.[912] However, some surveillance experts claim that large organisations remain relatively unaccountable even though they engage in automated social sorting practices that directly affect the lives of those whose data are processed by them.[913]

Accountability is a form of resilience in a surveillance society. Despite or perhaps because of the secretiveness of intelligence agencies, accountability becomes problematic. Indeed, it undermines democracy. In the UK, a former government minister revealed that the Cabinet was not told of the PRISM or TEMPORA programmes. He argued that the lack of information and accountability showed that "the supervisory arrangements for our intelligence services need as much updating as their bugging techniques".[914]

There have been calls for change from even within the intelligence community. A former member of Parliament's intelligence and security committee, Lord King, a former director of GCHQ, Sir David Omand, and a former director general of MI5, Dame Stella Rimington, have questioned whether the agencies need to be more transparent and accept more rigorous scrutiny of their work. A former legal director of MI5 and MI6, David Bickford, said Britain's intelligence agencies should seek authority for secret operations from a judge rather than a minister because public unease about their surveillance techniques is at an all-time high.[915]

The aforementioned House of Lords committee recommended, inter alia, mandatory use and publication of privacy impact assessments of surveillance systems:

> We recommend that the Government amend the provisions of the Data Protection Act 1998 so as to make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment (PIA) prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing. The Information Commissioner, or other independent authorities, should have a role in scrutinising and approving these PIAs. We also recommend that the Government—after public consultation—consider introducing a similar system for the private sector.[916]

Unfortunately, this recommendation has remained only partly implemented. Government departments are now obliged to conduct PIAs;[917] however, the ICO does not have a role in scrutinising and approving the PIAs. Hence, the quality of PIAs is highly variable. Although

---

[912] Regan, Priscilla, *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, 1995. See also Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield Publishers, Lanham, MD, 2002.

[913] Lyon, op. cit., 2009.

[914] Hopkins, Nick, and Matthew Taylor, "Cabinet was told nothing about GCHQ spying programmes, says Chris Huhne", *The Guardian*, 6 Oct 2013.
http://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne.

[915] Ibid.

[916] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, Volume I: Report, 2nd Report of Session 2008–09, The Stationery Office, London, 6 Feb 2009, p. 104.

[917] See Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008, Section I, 4.4: All departments must "conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews".
http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf. Gateway reviews are undertaken by an independent team of experienced people and carried out at key decision points in government programmes and projects to provide assurance that they can progress successfully to the next stage.

government departments report that they are conducting PIAs, few see the light of day.[918] Although some consult the ICO, most do not. The UK government has not implemented the recommendation about "a similar system for the private sector", although the proposed European Data Protection Regulation would make PIAs (or DPIAs, as the Commission calls them) mandatory for any organisation, public or private, where "processing operations present specific risks to the rights and freedoms of data subjects".[919]

The House of Lords also recommended various measures to improve oversight, e.g., as follows:

> We recommend that a Joint Committee on the surveillance and data powers of the state be established, with the ability to draw upon outside research. Any legislation or proposed legislation which would expand surveillance or data processing powers should be scrutinised by this Committee.[920]

Others have recommended more detailed oversight measures. For example, Roger Clarke has stated that "Because of the scope for significant harm to important personal, social, economic and/or political values, it is essential that proposals for surveillance schemes be subject to evaluation." He has also identified several essential characteristics of the evaluation process:

- justification and proportionality must be demonstrated for all intrusive aspects of the scheme
- details of the proposal must be sufficiently transparent that the evaluation can be undertaken
- the process must be consultative or participative, including representatives of and advocates for the interests of the categories of individuals affected by it
- unavoidable negative impacts and implications must be the subject of mitigation measures
- after a scheme is implemented, it must be subject to review
- depending on the outcomes of the review, the scheme may be approved for continuation unchanged, but more commonly must be subject to adjustment or withdrawal.[921]

Transparency, accountability and legality alongside an active civil society are the key ingredients of a functioning democracy. Civil society needs adequate resources to engage with democratic structures. If they have adequate resources, they sometimes achieve results and are able to roll back existing surveillance infrastructures, as happened in the case of the Birmingham Project Scheme, whereby social activists were able to have their voices heard, which resulted in the removal of more than 200 CCTV cameras installed in largely Muslim areas of the city.[922]

---

[918] Trilateral Research & Consulting, Privacy impact assessment and risk management, Report for the Information Commissioner's Office, 4 May 2013. http://ico.org.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/pia-and-risk-management-full-report-for-the-ico.pdf. See also Wright, David, Kush Wadhwa, Monica Lagazio, Charles Raab and Eric Charikane, "Integrating privacy impact assessment in risk management", *International Data Privacy Law*, Vol. 4, No. 2, June 2014, pp. 155-170.

[919] See Article 33 of European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

[920] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, Volume I: Report, 2nd Report of Session 2008–09, The Stationery Office, London, 6 Feb 2009, p. 108.

[921] Clarke, Roger, "The Resilience of Society in the Face of Surveillance", Xamax Consultancy Pty Ltd, 5 Feb 2013. http://www.rogerclarke.com/DV/IRISSR.html

[922] BBC News, "Birmingham Project Champion 'spy' cameras being removed", *BBC News,* 9 May 2011. http://www.bbc.co.uk/news/uk-england-birmingham-13331161

4.12.2 Explicit consent

James Rule comments that "what passes for consent to surveillance is often the only option for accessing things most people would consider elements of any normal life – a bank account, a credit card, or the opportunity to board an airplane". Companies, governments and others use various devices to gain nominal consent. Supermarkets, department stores and airlines use loyalty cards to gain the consumer's consent. In exchange for being awarded a thousand points and getting a free tea kettle, the consumer's consent means that the supermarket and other vendors with whom it is in alliance are able to target the consumer with online spam or junk mail as well as to build profiles of the consumer. Online, the consumer waives away personal data in exchange for a "free" program whereby s/he can more easily be tracked across cyberspace. In fact, since hardly anyone reads the terms and conditions or the privacy policy (if it can be found), the consumer has no idea what s/he is giving away.

Explicit consent in regard to mass surveillance systems is much more problematic, partly because governments and companies rarely seek anyone's consent for establishment of their surveillance systems or systems that can be used for surveillance. To obtain explicit consent in regard to planned surveillance systems, regulators should oblige organisations to conduct surveillance impact assessments (SIA) and engage a wide and representative range of stakeholders, including the public and consumer organisations, in the process and then submit the SIA report to the regulator for review and possible approval.

4.12.3 Other privacy principles

The notion and value of privacy have changed over time. In 1890, Brandeis and Warren regarded privacy as a right to be let alone, especially from those annoying journalists with their Kodak Brownie cameras.[923] The development of new and more intrusive technologies since then has undoubtedly circumscribed our notion and even value of privacy. We can assume the citizens of 1950 would be shocked by the intrusiveness of surveillance technologies today – of individuals being constantly monitored in physical and cyber space, of their person and behaviour being constantly monitored, of their having relinquished their date of birth, their fingerprints, retinal scans and DNA to governments and corporations. However, today's citizens accept these intrusions as the cost of living. Privacy is a much diminished right.

Privacy principles are important because they help to make more concrete what is meant by privacy and where lines against undue intrusions should be drawn. Thus, regulators should ensure that surveillance systems respect privacy principles, for example, those listed in ISO 29100 and/or those referenced in the proposed EU General Data Protection Regulation. However, those "privacy" principles are data protection principles. Privacy is more than data protection. Roger Clarke identified four categories of privacy in the mid-1990s, including privacy of the person, privacy of behaviour and privacy of communications.[924] Finn, Wright and Friedewald added privacy of location and space ("locational privacy"), privacy of

[923] The Eastman Kodak company introduce the Kodak Brownie in 1884. Warren and Brandeis published their famous article "The right to privacy" in the Harvard Law Review in 1890.
[924] Clarke, Roger, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997. http://www.rogerclarke.com/DV/Intro.html

association and groups and privacy of thought and feelings.[925] Surveillance drones, for example, capture behavioural privacy. Body scanners in airport intrude upon privacy of person (as do retinal scans and fingerprinting). Locational privacy means that people have the right to travel through physical and cyberspace without being tracked. People should have the right to meet or assemble anonymously with others. In short, surveillance intrudes upon other types of privacy, not only data protection. Thus, when assessing surveillance systems, regulators should assess the systems taking into account all types of privacy.

In a paper on the importance of principles in regulating surveillance, Charles Raab says surveillance may have consequences beyond those related to privacy "since surveillance may lead to discrimination and adverse decisions taken against individuals and groups in ways that cut across important values of fairness, equal treatment, and the rule of law, beyond any invasion of privacy itself".[926] He points out that "Depending upon the literature source, privacy either subsumes or is conducive to dignity, personality, selfhood, autonomy, social withdrawal, sociality, control over information, political engagement, liberty, and other values and interests… This makes it difficult to say what should be protected when 'privacy' is protected, and to what end(s) procedural principles should be oriented."[927] He also points out that "Many data protection systems around the world operate at both the level of broad principles and of more specific rules and guidance, while also using a wider range of instruments."[928] He cites UK privacy consultant Chris Pounder as finding the existing system for data protection deficient in terms of regulatory power and application. Pounder proposes nine principles for addressing whether privacy is protected against surveillance. In short form, they are:

- Principle 1: The justification principle (requiring an assessment of surveillance to justify it in terms of pressing social needs and measurable outcomes);
- Principle 2: The approval principle (requiring informed parliamentary scrutiny of legislation, and sometimes public debate);
- Principle 3: The separation principle (requiring authorisation of surveillance to be separated from carrying it out);
- Principle 4: The adherence principle (requiring surveillance staff to be managed, audited, and trained in proper procedures);
- Principle 5: The reporting principle (requiring the regulator to determine the keeping of surveillance records to ensure transparency and accountability);
- Principle 6: The independent supervision principle (requiring supervision of surveillance to be independent of government and empowered to investigate);
- Principle 7: The privacy principle (requiring an enforceable right to privacy of personal data and a right, in certain cases, to object to data processing);
- Principle 8: The compensation principle (requiring payment of compensation for unjustified damage, distress or detriment);
- Principle 9: The unacceptability principle (requiring cessation, steps towards compliance with principles, or parliamentary approval of non-compliance).[929]

---

[925] Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert and others (eds.), *European Data Protection: Coming of Age*?, Springer, Dordrecht, 2013.
[926] Raab, Charles D., "Regulating surveillance: The importance of principles" in Kirstie Ball, Kevin D. Haggerty and David Lyon (eds.), R*outledge Handbook of Surveillance Studies*, Routledge, Abingdon (UK), 2012, pp. 377-385 [p. 377].
[927] Raab, op. cit., 2012, p. 378.
[928] Raab, op. cit., 2012, p. 379.
[929] Raab, op. cit., 2012, pp.379-380. Raab cites Pounder, Chris, "Nine principles for Assessing Whether Privacy is Protected in a Surveillance Society", *Identity in the Information Society*, Vol. 1, No. 1, December 2008, pp. 1-22. http://link.springer.com/journal/12394/1/1/page/1

Raab emphasises that we should think about the consequences not only for individuals, but also for groups and for society generally. He casts some doubt on the adequacy of privacy principles for assessing surveillance schemes: "Many surveillance scholars doubt the efficacy of traditional or revised high-level principles of individual privacy protection as instruments for countering excessive surveillance and combating inequality between individuals, groups or categories of people, even where principles are embodied in legal regimes that specify rules. Instead, privacy is only a lever for prying open a much broader set of issues concerning citizenship, human rights and civil liberties."[930] Be that as it may, surveillance systems should be assessed with regard to its impacts on privacy – as well as other values.

Finally, anonymity protects privacy. It also offers a strategy for countering surveillance, but anonymity as a value seems to be diminishing even as the practical challenge of achieving anonymity is increasing.

4.12.4 Demarcating boundaries for surveillance

"The state should not feel itself entitled to know, see and memorise everything that the private citizen communicates. The state is our servant."[931]

Opposition, led especially by civil society organisations, but supported by the Conservatives and Liberal Democrats, led to the shelving of the Labour government's plans for a national identification card system in the UK. In the next government, the coalition of Conservatives and Liberal Democrats, opposition from the Liberal Democrats led to the shelving of the so-called "snooper's charter", legislation in the UK for implementing the EU Data Retention Directive.

These are examples of where public antipathy led to the drawing of lines – measures proposed by the government, but ultimately withdrawn because of popular opposition. These might suggest that control sometimes can be restored to the people. But instances such as these are the exception rather than the rule. To exercise some control over surveillance, to make government responsive to the will of the people, Bart Jacobs suggests five guidelines which he summarises as follows: "'select before you collect', 'decentralised storage of personal information', 'revocable privacy', 'attributes instead of identities', and 'reactive, non-proactive policing'."[932]

Select before you collect – Traditionally in a state of law one first has to become a 'suspect' before law enforcement authorities can undertake surveillance such as phone tapping. However, this order has been reversed and now information is collected first (about everyone), and subjects to be investigated are selected later. However, Jacobs favours the traditional approach.

Decentralised data storage – Centralised databases full of privacy sensitive information may be attractive for the database owners (or the authorities), but are not necessarily attractive for the subjects involved. New models and architectures are needed to handle such sensitive information, together with the political will and societal pressure to introduce them.

---

[930] Raab, op. cit., 2012, p. 384.
[931] Hopkins, Nick, and Matthew Taylor, "Cabinet was told nothing about GCHQ spying programmes, says Chris Huhne", *The Guardian*, 6 Oct 2013.
http://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne
[932] Jacobs, op. cit., 2009, p. 20.

Revocable privacy – The essence of revocable privacy is to design systems in such a way that no personal information is collected centrally, unless a user violates a pre-established policy... Privacy protection is thus not an add-on but is built deeply into the architecture of the system, and does not rely on legal or procedural safeguards that can be changed or circumvented relatively easily.

Attributes instead of identities – Many forms of authorisation do not require identification (and authentication), but only "attributes", such as being over 18, having a valid ticket, being a citizen of a particular country, and so forth.

Reactive policing only – There is pressure to make police work more proactive. This is uncontroversial when it comes to advising on safety precautions in homes, but active use of pattern-based data mining and developing personal profiles of all citizens is a different matter…. intelligence services should be allowed to use pattern-based data mining, for their restricted task, but police forces should not.[933]

Jacobs also suggests that some updating of legislation might be necessary.

> An important aspect of (European style) privacy laws is that people have the right to inspect what information on them is stored, and to require correction or even deletion under certain circumstances. These laws were written at a time when data mining was still in its infancy. It is not clear whether the right to inspection only applies to the stored personal data itself, or also to the derived personal profiles, or even to the selection mechanisms that are used in data mining.[934]

He suggests that people should have access, not only to their personal data, but also to the derived profiles. These guidelines, if implemented, would also be good examples of drawing lines – i.e., lines that governments and companies would not be permitted to cross.

4.12.5 Awareness and communication

Awareness and communication are important elements of resistance and resilience. If we do not know who is operating a surveillance systems or the extent of surveillance, then it is not possible to resist or to be resilient.

Raising awareness is a resilience measure. If the public is not aware of surveillance activities, it cannot judge whether such activities are acceptable, whether they are justified in the public interest. Fortunately, there have been various reports and news articles that have raised public awareness of surveillance. The Snowden revelations especially have generated a huge number of stories in the media and have been instrumental in raising public awareness about the extent of surveillance more than any other measure. Even before the Snowden revelations, other events helped raise public awareness. Former Information Commissioner Richard Thomas's warning that Britain may be "sleepwalking into a surveillance society" and publication of the SSN report in 2006 generated a great deal of coverage in the media and prompted headlines about "Big Brother Britain".[935] The Google Street View cars received a lot of attention, often negative, especially in Germany. When it was discovered that the

[933] Jacobs, op. cit., 2009, pp. 29-32.
[934] Jacobs, op. cit., 2009, p. 26.
[935] House of Commons Home Affairs Committee, *A Surveillance Society?*, Fifth Report of Session 2007–08, Volume I, The Stationery Office, London, 8 June 2008, p. 15.

vehicles were also capturing wireless network data, media interest spiked again. Google's data mining e-mail content in its Gmail service also prompted a lot of media attention, as did Facebook's trawling through users' data that was supposedly inviolate. Hence, the media has performed a reasonably good job in promoting public awareness of the ubiquity of surveillance in our (west European, North American) societies.

As another awareness-raising measure, the House of Commons surveillance report recommended that "The Information Commissioner should lay before Parliament an annual report on surveillance."[936] It also recommended "The Home Office should take every opportunity to raise awareness of how and why the surveillance techniques provided for by the Regulation of Investigatory Powers Act might be used." However, as the Home Office is responsible for many surveillance activities, this seems a bit like putting the fox in charge of the chickens. Indeed, Chris Huhne, the Cabinet minister, who said the UK national security council was kept in the dark about the PRISM and TEMPORA programmes, questioned whether the Home Office deliberately misled Parliament over the surveillance capabilities of GCHQ.[937] Thus, relying on government to inform the public about the amount of surveillance taking place is not going to work.

Whistle-blowers, such as Edward Snowden, and the news media play vital roles in raising public awareness of surveillance. The Snowden revelations resulted in the European Parliament's endorsed a tougher Data Protection Regulation in October 2013 than might otherwise have been the case. Article 42 (1), the so-called anti-FISA clause, had been dropped between the unofficial version of the proposed Regulation leaked in early December 2011 and the official version released on 25 January 2012. But following the Snowden revelations, the European Parliament's LIBE committee re-instated the clause.

4.13 INDIVIDUAL MEASURES

This section looks at some measures individuals could take to build resilience in surveillance societies.

4.13.1 Resistance

Individuals may be able to resist surveillance by retreating from society, by decamping to a remote or rural area beyond the purview of CCTV cameras, but the reality is that retreatism is not possible if one wishes to live in an urban society. In any event, if one does retreat (withdraw) to a remote area, it is possible that such a retreat might only raise the suspicions of the surveillant and thereby stimulate greater surveillance.

In any event, even citizens in non-urban society, such as those living in the countryside, are subject to extensive forms of surveillance but these may manifest themselves in different ways. For example, other villagers may take the place of cameras.

Assuming most people are not latter-day Robinson Crusoes, there are some measures that an individual can take to resist or thwart the pervasiveness of surveillance, such as those described by Gary T. Marx, as noted before.[938] In addition to those suggested by Marx, there

[936] Ibid, p. 7.
[937] Hopkins, op. cit., 2013.
[938] Marx, Gary T., "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 369-390. Marx further elaborated upon resistance strategies in Marx, Gary T.,

are other measures for thwarting mass surveillance, for example, individuals can install Adblock[939] or other anti-malware software on their computers to block unwanted cyber spiders from gathering personal data from their computers that companies might otherwise use to target them with personalised advertising.

Civil society organisations can act as a proxy for (and support) individuals in campaigns against surveillance. The US Electronic Privacy Information Center (EPIC), a privacy advocacy group based in Washington DC[940], uses class action suits as a form of individual resistance. Class action suits may become a European phenomenon too. On 11 February 2014, Germany's Federal Minister of Justice and Consumer Protection announced that consumer rights organisations will soon be able to sue businesses directly for breaches of German data protection law. The proposed new law that would enable such law suits would bring about a fundamental change in how German data protection law has been adopted. Until now, only the affected individuals and Germany's criminal prosecutors and data protection authorities had legal standing to sue businesses for breaches of data protection law. With the new law, legal proceedings against businesses for data protection breaches are expected to become more common in Germany.[941]

An interesting example of civil society organisations collaborating in efforts to raise awareness and to lobby against mass surveillance is "The Day We Fight Back against mass surveillance" campaign which, as of February 2014, had garnered support from more than 360 organizations in more than 70 countries of its "International Principles on the Application of Human Rights to Communications Surveillance". The 13 principles aim to establish the human rights obligations of any government conducting surveillance. According to its website, the principles "are the core of an international movement to compel all states to stop the mass spying of the innocent. The Principles are already being used in national campaigns and international pressure to reign in spies including the NSA."[942] The campaign was also open to support from members of the public and, as of February 2014, the website said it had gathered about 250,000 people (and counting).

4.13.2 Use of privacy-enhancing technologies

According to documents leaked by Edward Snowden, the NSA and GCHQ have been collecting data transmitted "in the clear" by applications, games and social networks such as Angry Birds, Facebook, Flickr, Flixster, Google Maps, LinkedIn, Photobucket and Twitter. In addition to the vast amount of personal data being transmitted unencrypted across open cellular networks by the apps themselves, the agencies were reportedly able to get even more intrusive information — including a person's religion, sexual orientation and marital status — from third-party advertising networks that placed ads in smartphone apps.[943]
To hinder such intrusions, individuals should employ privacy-enhancing technologies (PETs). PET can be categorised according to their functionalities and the actors involved in their use.

"A Tack in the Shoe and Taking off the Shoe: Neutralization and Counter-neutralization Dynamics", *Surveillance & Society*, Vol. 6, No. 3, pp. 294-306.

[939] https://adblockplus.org/en/firefox

[940] http://epic.org/

[941] Privacy and Information Security Law Blog, "German Ministry Moves on Privacy Litigation", Hunton & Williams LLP, 11 Feb 2014. https://www.huntonprivacyblog.com/2014/02/articles/german-ministry-moves-privacy-litigation/

[942] https://thedaywefightback.org/international/

[943] Wagenseil, Paul, "7 ways to stop NSA spying on your smartphone", *NBC News*, 29 Jan 2014. http://www.nbcnews.com/technology/7-ways-stop-nsa-spying-your-smartphone-2D12008815

The main classes of functionalities are information hiding (e.g., anonymisation, encryption, etc.), information management (subject privacy policies, user interfaces, etc.), transparency (dashboards, controller privacy policies) and accountability (traceability, log management, etc.). As far as the actors involved are concerned, we can identify three main categories: the subject himself, trusted third parties and pairs. The categories of actors required to deploy a tool can have a great impact on its usability and on the type of protection and trust provided by the tool. The role of the subject is also a critical aspect which requires careful thinking. It is related to the notion of consent, its value for privacy protection but also its limitations and the risks of relying too much on it.[944]

From time to time, the news media provide some helpful advice on steps that can be taken to make it more difficult to surveil what individuals are doing. For example, NBC News recently suggested several measures that can be taken while playing games on smart phones:

1. Put your phone into airplane mode while playing games.
2. Use a virtual private network (VPN) while connecting to the Internet.
3. Don't post on social media accounts while connected to cellular data networks.
4. Install HTTPS Everywhere.[945]
5. Turn off Wi-Fi, GPS and geolocation on your phone.
6. Turn off cellular data connections.
7. Get rid of the smartphone.[946]

4.14 SOCIETAL MEASURES

An individual may dissent against unruly surveillance practices, but it is only when the individual is joined by thousands of peers that societal pressure on politicians or CEOs becomes noticeable or even effective. Widespread opposition to the last Labour government in the UK led to the death of the ID scheme the implementation of which had already begun when the coalition government came to power and dropped the scheme as they had promised. Similarly, widespread opposition in the UK to the so-called "snooper's charter" led to the cancellation of that scheme that would have seen retention of metadata on all telephone calls in the UK for up to two years.

We should distinguish and understand the differences between individual and societal measures. The two are generally different in terms of their objectives and successes. An individual response to surveillance might be putting plastic bags over CCTV cameras whereas a manifestation of societal resilience might be opinion polls showing that the citizenry is generally opposed to unpopular measures such as the introduction of ID cards in the UK.

Advocacy groups, such as Privacy International, Big Brother Watch, Statewatch EDRi-gram, etc., frequently generate stories in the media drawing to the attention of the general public the intrusiveness of surveillance measures.

Sometimes individual measures can have societal impacts. Individual initiatives to marshal public opinion via the Change.org polls have sometimes had good results.

---

[944] This paragraph comes from an abstract prepared by Daniel Le Metayer for a chapter in a forthcoming book: Wright, David, and Paul De Hert (eds.), *Enforcing Privacy*, Springer, Dordrecht, 2015.

[945] HTTPS Everywhere is a browser plugin for Firefox, Chrome and Opera desktop browsers provided free by the Electronic Frontier Foundation. https://www.eff.org/https-everywhere

[946] Wagenseil, Paul, "7 ways to stop NSA spying on your smartphone", *NBC News*, 29 Jan 2014. http://www.nbcnews.com/technology/7-ways-stop-nsa-spying-your-smartphone-2D12008815

4.14.1 Correcting power asymmetries

Monahan states that "the most democratic and socially empowering designs (of spaces, products, or technological systems) are those that work to correct power asymmetries. Often these are designs that are explicitly intended to include social groups that have been historically marginalized or discriminated against… The same insight could be applied to the design of surveillance infrastructures – to produce technological sensing and control devices that minimize power asymmetries to the benefit of individuals and the empowerment of a democratic citizenry."[947]

There are various ways of correcting power asymmetries. Electing a new government may not be a game-changer if the new government continues the same surveillance policies and practices as its predecessor (e.g. US President Obama continued or even expanded upon the initiatives of George Bush).

One whistle-blower, Edward Snowden, upset established orders. His revelations strengthened the resolve of MEPs in the European Parliament to strengthen the proposed General Data Protection Regulation and to produce a strong report with strong recommendations on the NSA revelations. The German and French promoted the idea of a European cloud alternative to those services offered by US providers such as Google, Amazon, Microsoft, etc. These same providers and others in their cohort have lobbied President Obama to cut back on mass surveillance because they perceived it to be hurting their business. The Snowden revelations prompted Germany and Brazil to co-operate in producing a resolution which was adopted by the UN General Assembly and which also called for better oversight of the intelligence communities. More people are using encryption and adopting other privacy-protecting measures.

These and other events show that to correct power asymmetries is very difficult, but a shock (e.g., the Snowden revelations) that receives significant media attention may help to create enough public agitation that it can prompt a correction in power asymmetries.

4.14.2 Public opinion polls

Although politicians often say that the only poll that counts is the one on election day, the fact is that politicians take regular soundings of their constituents and pay attention to other polls. They may choose not to act on the results of a public opinion survey, but they do pay attention them nevertheless. Thus, an informed electorate may express its rejection of mass surveillance in soundings that may make politicians, if not corporate oligarchs, consider whether it is in their own interests in continuing the development, deployment or maintenance of particular surveillance systems.

However, not all public opinion surveys are conducted rigorously, while some opinion surveys may be deliberately designed to elicit a particular response. An extensive review of opinion surveys can be found in a report of the EC-funded PRISMS project.[948]

[947] Monahan, op. cit., p. 103.

[948] http://prismsproject.eu. The PRISMS project is distinct from and should not be confused with the NSA programme, under which the agency was collecting e-mails, Internet phone calls, photos, videos, file transfers and social-networking data from Google, Facebook, Apple, YouTube, Skype, Microsoft and PalTalk

4.14.3 An activist press

An activist press is an essential safeguard against the intrusions of, especially, state-sponsored surveillance. The press play a vital role in raising public awareness about how extensive surveillance has become.

Many media outlets face financial pressures and may not have the resources for investigative journalism and rigorous reporting. Competitive envy may deter some newspapers from reporting the exclusives that competitors have broken. In the UK, for example, few newspapers have referred to the stories broken by The Guardian.

Furthermore, an activist press depends upon constitutional protections of the right to freedom of expression. Such a right does not exist in the UK and, as described in Luke Harding's book *The Snowden Files*, governments may try to intimidate the press to force it to refrain from reporting stories that the government may deem to damaging to the national interests (and especially to the government's interests, which are not necessarily the same thing).

4.15 CONCLUSIONS

There is no doubt that "we" (the public in Western Europe and elsewhere) live in a surveillance society. The Snowden revelations have served to make plain just how pervasive surveillance by the intelligence agencies has become. Although the Snowden files were a revelation to most people, they were presaged by other investigative journalists, especially James Bamford[949] and Duncan Campbell (who broke the ECHELON spy satellite story[950]).

Although the Snowden revelations have principally concerned surveillance by the NSA, GCHQ and other intelligence agencies, big companies such as Google, Facebook, Amazon, Microsoft and others, have also engaged in mass surveillance in order to better target advertising and grow their revenues. Personal data has become the fuel of governance and the modern economy. Such is one way companies and government attempt to excuse their activities. In reality, corporate surveillance is just as insidious as that conducted by the intelligence agencies and other wrong-doers in China, Russia and North Korea, among other countries.

With the development of the so-called Internet of Things and other new technologies, surveillance will undoubtedly become more pervasive than it already is. Such pervasive surveillance undermines privacy, which is a fundamental right in Europe and which is widely regarded as a cornerstone of democracy.[951] Our nominal democracies are simulacrums, much

---

[949] Bamford has written extensively about the NSA's surveillance activities. See especially Bamford, James, *The Shadow Factory*, Anchor Books, New York, 2009.

[950] Campbell has written numerous articles about the ECHELON system. His earliest contribution was "Somebody's listening", published in *The New Statesman*, 12 August 1988. His stories eventually led to an inquiry by the European Parliament. See Schmid, Gerhard, On the existence of a global system for the interception of private and commercial communications (ECHELON interception system), 2001/2098(INI), European Parliament: Temporary Committee on the ECHELON Interception System, 11 July 2001.

[951] Brazilian President Dilma Rousseff told the United Nations that "Without the right of privacy, there is no real freedom of speech or freedom of opinion, and so there is no actual democracy." Quoted in Lynch, Colum, "Brazil's president condemns NSA spying", *The Washington Post*, 24 Sept 2014. http://www.washingtonpost.com/world/national-security/brazils-president-condemns-nsa-spying/2013/09/24/fe1f78ee-2525-11e3-b75d-5b7f66349852_story.html The Supreme Court of Canada has stated that "society has come to realize that privacy is at the heart of liberty in a modern state ... Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual". R. v. Dyment

like a zombie is a simulacrum of a free-thinking, alive human being. Our democracies are being supplanted by a new kind of totalitarianism or tyranny, which is different from the totalitarian regimes of East Germany or the Soviet Union in days gone by or the society depicted by George Orwell in *1984*. Haggerty and Samatas, with reference to Ben Hayes, a contributor to their book, opine that "as surveillance measures are increasingly justified in terms of national security, a shadow "security state" is emerging – one empowered by surveillance, driven by a profit motive, cloaked in secrecy and unaccountable to traditional forms of democratic oversight".[952]

Today's surveillance society is more like that depicted in the Steven Spielberg film, *Minority Report*. But even that film, set in the future, does not adequately depict today's surveillance society. In today's surveillance society, intelligence agencies conduct mass surveillance not only to catch terrorists, but eavesdrop on nominal allies and friends in order to gain an advantage in trade negotiations and to spy on competitors. It is apparent that, despite the criticism from the news media, academics, industry and advocacy organisations, the US government has no intention of stopping its mass surveillance of people in the US and other countries.[953] It is likely that there are corporate and state surveillance systems of which we are unaware.

Surveillance has a deleterious effect on privacy and other human rights. Today's surveillance societies are marked by control, manipulation and a breakdown of trust. Governments and corporation try to control and manipulate citizen-consumers in a variety of ways for a variety of purposes. Citizens are (fortunately) not stupid. Some of their control and manipulation activities are perceived as such and lead to a breakdown in trust. Opinion polls show just how little citizens trust their governments. An October 2013 survey of American, Canadian and British adults by Angus Reid Global indicated that people distrust their national leaders to be good guardians of the information gathered or to restrict its use to national security purposes.[954] When asked whether they trusted their national government to be "a good guardian of citizens' personal information", 60 per cent of Americans and 64 per cent of Britons and Canadians said they had "not that much trust" or "no trust at all". In each country polled, at least 75 per cent of respondents described the issue of government surveillance of the public's Internet communications as "very" or "quite" important to them (US: 77%, Canada: 78% UK: 82%). Asked to assume their national government is routinely conducting electronic surveillance of the general public, 60% of Americans and Canadians described this as "unacceptable", while Britons were more split, (52% unacceptable versus 48% acceptable). Only one in five respondents believe information gathered by governments will be used for "strictly national security/anti-terrorism efforts" (US: 21%, UK: 19%, Canada: 18%).

---

(188), 55 D.L.R. (4th) 503 at 513 (S.C.C.). Also: "Without privacy, it is much harder for dissent to flourish or for democracy to remain healthy and robust. Equally, without privacy the individual is always at the mercy of the state, forced to explain why the government should not know something rather than being in the position to demand why questions are being asked in the first place." Goold, Benjamin J., "Surveillance and the Political Value of Privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009.

[952] Haggerty and Samatas, op. cit., p. 11.

[953] The White House, "Remarks by the President on Review of Signals Intelligence", Office of the Press Secretary, Washington, DC, 17 Jan 2014. http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence. See also Nelson, Steven, "Obama Praises NSA, Trashes Edward Snowden", *US News & Business Report*, 17 Jan 2014. http://www.usnews.com/news/articles/2014/01/17/obama-praises-nsa-trashes-edward-snowden

[954] Angus Reid Global, "More Canadians & Britons view Edward Snowden as 'hero' than 'traitor', Americans split", 30 Oct 2013. http://www.angusreidglobal.com/polls/48837/more-canadians-britons-view-edward-snowden-as-hero-than-traitor-americans-split/

A lack of trust in our institutions is also invidious to democracy. It betrays a lack of solidarity and social cohesion. A surveillance society is a dysfunctional society. (Other signs of a dysfunctional society are growing and extreme inequities, for example, between the richest and poorest segments.) A surveillance society is about power. Surveillance systems are instruments of the status quo, of helping those with great power to maintain their control over those with little power. Apologists for today's surveillance society can point to sousveillance as an indication of how the cost of surveillance technologies has dropped so that even ordinary citizens can surveil police efforts to maintain control in volatile demonstrations. But in reality, as Coleman and McCahill point out, such sousveillance has virtually no effect in altering existing power relationships.[955]

In surveillance societies, resilience and resistance become necessary so that citizen-consumers are not completely overwhelmed. Academics have questioned the definition of both terms, partly because the terms themselves have become overused in a wide variety of contexts. Be that as it may, we find utility in both terms. We regard resilience in surveillance societies as a capacity of citizen-consumers to cope with the prevalence of surveillance. Although one can draw a distinction between resilience and resistance, they overlap to some degree. Resistance in a surveillance society can take many forms, some legal and some not. Resistance may involve spray-painting CCTV cameras, but may also involve the use of privacy-enhancing technologies aimed at thwarting governments and companies from tracking our activities in cyberspace or switching off or abandoning the use of smart phones in physical space. Resistance can be active opposition to surveillance regimes. Resistance, while different from resilience, at least in the sense of coping, can also be regarded as an element in resilience. Investigative reporting of surveillance activities and depicting surveillance societies in films such as *The Conversation*, *Minority Report*, *Enemy of the State*, *Lives of Others* and so on can also be regarded as manifestations of resilience.

Resilience, like accountability, has an ambivalent, even dangerous edge, i.e., both terms can suggest an acceptance of the status quo. But given how extensively surveillance has seeped into the body politic as well as our own physical, mental and attitudinal states, we do not want acceptance.

Georgios Kolliarakis argues that "The current predominance of surveillance detection technology research seems to be on collision course with competing objectives, such as in policies of non-discrimination or inclusion of civilians in the European societies."[956] Furthermore, the so-called "societal dimension" is frequently reduced to the issue of acceptance of new security technologies by the public.[957] He notes that the European Commission acknowledges "'societal resilience' depends on the free will of informed citizens as much as on the quality of technical systems and on business continuity capabilities of companies and administrations."[958] While engaging stakeholders is a generally a good thing, Kolliarakis notes that "the engagement of public policy makers, scientists and researchers, developers and operative end-users does not always bear the expected fruits".[959] He cites resilience pioneer Jon Coaffee who concludes that "resilience is most effective when it

[955] Coleman and McCahill, op. cit., 2011, p. 147.
[956] Kolliarakis, op. cit. 2013, p. 9.
[957] Kolliarakis, op. cit. 2013, p. 10.
[958] European Commission, A European Security Research and Innovation Agenda – Commission's initial position on ESRIF's key findings and recommendations, COM (2009) 691 final, Brussels, 2009, p. 3.
[959] Kolliarakis, op. cit. 2013, p. 14.

involves a mutual and accountable network of public institutions, agencies and individual citizens working in partnership towards common goals within a common strategy."[960]

Individuals and societies need to take measures to curtail surveillance. Whistle-blowers and investigative journalists can help influence public opinion which may in turn influence politicians and corporate practices, but this should not be overstated. Secret laws and orders should not be permitted. Much improved oversight, especially by regulators, is a prerequisite for reining in the pervasiveness of surveillance. James Rule argues that "Any system that monitors individual lives, and enables institutions to intervene in those lives, thus demands extreme prudence."[961] He adds that "The new default condition for public policy should be: no government surveillance without meaningful individual consent or legislative authorization." [962] With regard to the private sector, he says "a parallel precept should apply: no use of personal data for institutional surveillance without meaningful, informed consent from the individual." [963] Surveillance impact assessments can help, but should not be seen as *the* solution, merely as one arrow in a quiver of multiple means and efforts and approaches to curtail mass surveillance.

References

Aradau, Claudia, "The myth of preparedness", *Radical Philosophy*, RP 161, May/Jun 2010. http://www.radicalphilosophy.com/commentary/the-myth-of-preparedness

Béné, Christophe, Rachel Godfrey Wood, Andrew Newsham and Mark Davies, "Resilience: New Utopia or New Tyranny? Reflections about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes", IDS Working Paper, Vol. 2012, No. 405, CSP Working Paper Number 006, Institute of Development Studies, September 2012.

Chandler, David, "Editorial", *Resilience: International Policies, Practices and Discourses*, Vol. 1, No. 1, March 2013.
http://www.tandfonline.com/doi/pdf/10.1080/21693293.2013.765739

Clarke, Roger, "The Resilience of Society in the Face of Surveillance", Xamax Consultancy Pty Ltd, 5 Feb 2013. http://www.rogerclarke.com/DV/IRISSR.html

Coleman, Roy, and Michael McCahill, *Surveillance & Crime*, Sage, London, 2011.

Cowell, Alan, "Cameron Criticizes The Guardian for Publishing Secrets", *The New York Times*, 16 Oct 2013. http://www.nytimes.com/2013/10/17/world/europe/cameron-criticizes-the-guardian-for-publishing-secrets.html?src=un&feedurl=http%3A%2F%2Fjson8.nytimes.com%2Fpages%2Fbusiness%2Fmedia%2Findex.jsonp

[960] Coaffee, Jon et al., *The Everyday Resilience of the City: How Cities Respond to Terrorism and Disaster*, Basingstoke, 2009, p. 3.
[961] Rule, op. cit., 2007, p. 184.
[962] Rule, op. cit., 2007, p. 195.
[963] Rule, op. cit., 2007, p. 196.

Hamel, Gary, and Liisa Välikangas, "The Quest for Resilience", *Harvard Business Review*, September 2003.

House of Commons Home Affairs Committee, *A Surveillance Society?*, Fifth Report of Session 2007–08, Volume I, The Stationery Office, London, 8 June 2008.

House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, Volume I: Report, 2nd Report of Session 2008–09, The Stationery Office, London, 6 Feb 2009.

Levine, Simon, Adam Pain, Sarah Bailey and Lilianne Fan, "The relevance of 'resilience'?", HPG Policy Brief 49, Overseas Development Institute, London, September 2012. www.odihpn.org

Longstaff, P.H., *Security, Resilience, and Communication In Unpredictable Environments Such as Terrorism, Natural Disasters and Complex Technology*, Center for Information Policy Research, Harvard University, Cambridge MA, Nov 2005.
http://pirp.harvard.edu/pubs_pdf/longsta/longsta-p05-3.pdf

Lyon, David, "Surveillance, Power, and Everyday Life", in Robin Mansell, Chrisanthi Avgerou, Danny Quah and Roger Silverstone (eds.), *The Oxford Handbook of Information and Communication Technologies*, Oxford University Press, 2009, pp. 449-472.

Marx, Gary T., "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 369-390.

Marx, Gary T., "A Tack in the Shoe and Taking off the Shoe: Neutralization and Counter-neutralization Dynamics", *Surveillance & Society*, Vol. 6, No. 3, pp. 294-306.

Monahan, Torin, "Surveillance policies and practices of democratic governance", in Kevin D. Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, Abingdon, 2010.

Nathan, Andrew J., "Authoritarian Resilience", *Journal of Democracy*, Vol. 14, No. 1, January 2003, pp. 6-17.

Neocleous, Mark, "Resisting resilience", *Radical Philosophy*, RP 178, March/April 2013.
http://www.radicalphilosophy.com/commentary/resisting-resilience

Organization for Economic Co-operation and Development, *Concepts and Dilemmas of State Building in Fragile Situations: From Fragility to Resilience*, OECD, Paris, 2008.

Reid, Richard, and Linda Courtenay Botterill, "The Multiple Meanings of 'Resilience': An Overview of the Literature", *Australian Journal of Public Administration*, Vol. 72, No. 1, March 2013, pp. 31-40.

Surveillance Studies Network, *A Report on the Surveillance So*ciety, For the Information Commissioner, September 2006.

Walker, Jeremy, and Melinda Cooper, "Genealogies of resilience: From systems ecology to the political economy of crisis adaptation", *Security Dialogue*, Vol. 42, No. 2, 2011, pp. 143-160.

5 LESSONS LEARNED FROM WPS 3 – 5 WITH SPECIFIC REGARD TO RESILIENCE

In this section we review, analyse and synthesise the lessons learned from WPs 3 – 5 with specific regard to resilience. This will thus enable a comparison between the empirical findings of these WPs with the theoretical findings of Task 6.1 (review of resilience theory and state of the art). The results of this comparative analysis will feed into Task 6.3.

5.1 LESSONS LEARNED FROM WPS 3 – 5 WITH SPECIFIC REGARD TO RESILIENCE

5.1.1 Findings from WP3 – Case studies

Professor Kirstie Ball, Open University

WP3 presents case studies of three surveillance practices across Europe: ANPR, Credit Scoring and Neighbourhood Watch. These practices were chosen because they represent different institutional surveillant relationships: between citizens and the state (ANPR), citizens and the private sector (Credit Scoring) and citizens and each other (Neighbourhood Watch). This report examines how democratic resilience can be increased in the face of these pervasive surveillance practices. The theoretical premise for the case study is that while surveillance practices can be deployed to counter threats and risks and to prevent harm occurring, they also create potentially harmful consequences. The reliance of surveillance practices on proprietary information infrastructures can make surveillance processes non-transparent and unaccountable to democratic scrutiny. As the capacity to surveil bestows great power, it is vital that this power is wielded responsibly, ethically and with due respect to the law and human rights. The WP3 case studies examined the extent to which the focal surveillance practices created harms or were controversial, and the extent to which they intersected with democratic practices of governance, participation and engagement.

Three case studies were examined in different European countries. ANPR was examined in Belgium, Germany, Slovakia and the UK. Credit Scoring was examined in Austria, Hungary, Italy, Norway and the UK; Neighbourhood Watch was examined in Austria, Germany, Spain and the UK. The central finding is that increasing resilience to surveillance in Europe begins with increased public – and institutional – awareness of its harms and its benefits. For the watchers - those organisations in whose favour surveillance was deployed - surveillance produced several benefits. These benefits included better risk management, traffic law enforcement etc., which has almost made the watchers immune to recognising that harms may arise. Even though activist groups and the media have been working hard to highlight the harms associated with specific instances of ANPR (UK, Slovakia, Belgium), and credit Scoring (UK, Norway), changes in governance are also needed to limit the effect of those harms. The picture here is variable, as shown below.

ANPR resulted in some harms against which resilient strategies need to be formulated. The case studies found evidence that use of ANPR had circumvented and breached the rule of law, compromised rights and raised privacy issues. In the least regulated country, the UK, it had

been found to affect detrimentally the right to protest and had even deliberately been deployed in a racist manner by police in Birmingham following Project Champion. However, the situation in Slovakia extended the harms resulting from the surveillance practice. In an effort to avoid the economic losses imposed by road tolls, Slovakian truck drivers had taken to driving on smaller roads and thus affected the quality of life for the villages located on those roads. In the ANPR case, with the exception of Germany, very low engagement of the public was evident because of a lack of consistent regulation and signage, low levels of general media coverage and low engagement of data protection regulators with the practice. In relation to ANPR, in respect of its very significant harms, we observed different levels of governance which lagged behind technological capabilities. The first priority would be to harmonise governance through a European level directive. The gold standard developed in Germany, based on constitutional scrutiny and limitation of ANPR data collection would be a good starting point. Mandatory signage, enhanced DPA powers and the use of privacy by design in the tendering processes for ANPR systems would perhaps feature in this directive. The provision of figures proclaiming the effectiveness of ANPR systems in detecting crime should also be made available by law enforcement agencies.

The harms associated with credit scoring relate to administrative matters and highlight how this form of surveillance is explicitly part of a management process and hence subject to administrative errors. However, the case studies uncovered evidence of bank and legal staff abusing their position in relation to the sensitive financial data (Austria, Hungary). Similarly its location in the commercial sector meant that some unscrupulous organisations exploited it to facilitate lending money to customers who could ill-afford it and were financially illiterate (UK). Overall, this points to a problem in transparency and with the operation of the rule of law in relation to credit scoring (Italy, Hungary, Austria). The distributive justice aspects of credit scoring and its ability to delimit economic prosperity were noted in the UK and Norwegian cases particularly. With the exception of Norway and the UK, there was minimal public engagement and low awareness of the practice. The first issue to solve is the public's awareness of, and access to their own credit scoring data. While this is widely available in the UK and Norway, this is not the case in Austria, Italy and Hungary. Increasing transparency and accountability of financial institutions in relation to credit scoring data again could be initiated at the European level. Other countries could learn from the Norwegian model, which places the data protection authority at the heart of credit scoring and invests genuine powers in the courts to hear citizens' complaints about credit scoring practices. Following the credit crunch, demand for credit is now increasing across Europe and institutions should take this opportunity to inform consumers of their rights. Controversies associated with credit scoring appear in all of the case study countries, but in some cases the media have been slow to react, resulting in ill-informed consumers, and unaccountable, non-transparent financial institutions.

In the Neighbourhood Watch (NW) case studies, privacy was a relatively minor issue associated with the schemes' use of online and social media. The cultural and social significance of surveillance was far more powerful and generated strong sentiment towards it as a community safety idea (Austria, Germany, and Spain). In these cases surveillance processes became controversial as in addition to creating unhelpful links with the past, it was feared that they would present opportunities for extremists of all political colours. This was strongly observed in the German and Spanish cases.

The presence of NW-like organisations stigmatised particular spaces and focused on victimising those who were perceived as 'other' at that moment. It also challenged policing authorities who, at a community level, tread a fine line between too-little or too-much

intervention, leading to an increase in feelings of insecurity if crime appears to be increasing. Neighbourhood Watch is a special case; with the exception of the UK, it has developed outside the remit of law enforcement institutions. However, the experience of NW in the case study countries is simultaneously an example of community resilience and community breakdown. In an attempt to create community safety, its harms stem from frustration with 'the other' and insecurities related to community policing. The British example, with minimal regulation and a caring focus, shows how NW can succeed without the deep levels of mistrust and unpleasant associations which stem from authoritarian pasts. The community reaction Neighbourhood Watch in Austria, Germany and Spain represents how those societies have become resilient to the surveillance they suffered at the hands of authoritarian and fascist governments. Improved relations within communities as well as between communities and police would further strengthen this resilience. Frustrations with a low police presence as a result of funding cuts (among other things) point to how this surveillance practice is intertwined with public resourcing issues. Whilst it is inevitably difficult to prioritise resource deployment in the current public financial climate, it is always important for police to be connected with the communities that they serve.

Overall, the intersection between surveillance and democracy across the three case studies examined is varied. Patterns emerged which are associated with historical, legal, political, social and institutional factors. To a greater degree than ever before, surveillance processes intersect with and constitute the way in which we get things done. As consumption, communication, security and even democracy is done in this way – we need to question how transparency and accountability re-organise themselves - which will enable alternatives to emerge.

5.1.2 Findings from WP4 – Citizens and their attitudes to surveillance

Dr Reinhard Kreissl, Institute for the Sociology of Law and Criminology (IRKS)

The focus of WP 4 was on citizens' attitudes towards surveillance practices as an element of their everyday lives. About 300 exhaustive interviews were conducted in 5 countries, producing a database of approximately 1000 individual stories about surveillance, resilience and privacy (elicited from respondents). Country reports, based on media analysis and other data were compiled to account for national differences between the countries involved in the study. These countries were: Italy, United Kingdom, Germany, Slovakia, and Austria. Interview partners were recruited using different institutional entry points like police, consumer associations, labour unions, NGOs active in the field of (anti)-surveillance policy. For each country a control group of 20 respondents was recruited using snowballing techniques from random entries outside the institutional entry points for the recruitment of the target group.

The country reports show that the public debate about surveillance is very different in the countries involved. A number of general topics were analysed for a period of ten years for each country (such as the public debate about the EU data retention directive or the Google street view project; with regard to surveillance the activities of NGOs, media debate and public protest – if any – were documented). While, e.g. in Italy public debate about surveillance measures in public space (CCTV) did not produce a public controversy, except for the use of surveillance cameras in schools, the practices of tax authorities, looking into individual taxpayers' records seemed to have captured more critical attention. In Slovakia no

significant public debate about the dangers of surveillance has taken place. While a couple of NGOs attempt to get public attention about surveillance-related events (primarily the practices of national secret services) Google Street View as a commercial project was generally welcomed in this country. On the other hand a fierce debate about the so-called "cookie law" broke out in the UK. In general there seems to be a greater awareness with regard to specific surveillance related topics in the UK, while at the same time CCTV is widely accepted in British society. The country reports nicely demonstrate the variety of reactions towards surveillance across Europe: in some countries (e.g. Slovakia and Italy), the general public and media did not take up surveillance as an issue in the context of debates about fundamental rights and democracy. In other countries (e.g. Germany) there was considerable public arousal and protest against surveillance, whereas in Austria only few civil activists made it to the streets to protest against surveillance. The most elaborate debate took place in the UK, albeit with a focus on issues (the use of cookies by websites) that did not surface in other countries at all as a topic of debate. These country reports can be used to frame the more in-depth qualitative data obtained through interviews with citizens, trying to elicit their views on surveillance.

Taking citizens' perspectives as a starting point has a number of theoretical and methodological consequences, relevant to resilience. Concepts such as "surveillance", "privacy", or "resilience" are not common coinage for most of the European citizens most of the time. Except for situations where problems of surveillance score high on the political and media agenda (e.g. as triggered by the revelations of Edward Snowden on the practices of the NSA and CIA), surveillance, privacy, security, and resilience are not topical in managing everyday life for the average lay person. Of course, attitudes of citizens towards surveillance and resilience can be investigated, when confronting them with explicit questions, e.g. when conducting a survey on privacy and security. But obtaining a response upon reflection of a question and considering problems of surveillance and resilience on a daily basis and spontaneously are two different things.

Why is this distinction important? There are two important reasons to consider the difference between an elicited answer to a question and a spontaneous reaction. First, priming subjects with a cognitive frame, focussing on the problem of surveillance creates a mind-set where feelings of security and insecurity become topical. Once a person begins to reflect about her own security (e.g. because of being asked to do so) feelings of insecurity emerge. In everyday life ontological security is the default state of the individual and this state is not linked to any conscious or reflective attitude. The mental state of security is constitutively a by-product. It cannot be consciously created. This is the so-called security paradox, haunting all research on fear of crime: People tend to feel secure as long as they are not asked to reflect about their security. Of course there are a number of situations where feelings of insecurity emerge, but insecurity as a state of mind is the exception and not the rule. Second, in a longer, historical perspective surveillance has become a pervasive feature of everyday life, but this growth of encompassing surveillance in society proceeds in an incremental fashion without being noticed explicitly. Citizens are tied into a web of surveillance systems and practices in their daily walks of life without realizing, how this net is becoming slowly and continuously more and more dense. Investigating citizens' perspectives towards surveillance and resilience one has to consider that neither of these concepts are consciously represented in everyday understanding of lay people but nonetheless shape their daily routines in many different ways.

Taking an outside expert observer's perspective the pervasiveness of surveillance modern societies becomes immediately obvious. Citizens in modern Western societies have been

transformed into techno-social hybrids, tracked, located and watched, and their different daily activities are recorded, analysed and the results are used for a myriad variety of purposes by public and private actors. Getting access to goods and services requires multiple procedures of identification, using machine-readable tokens of identity (PIN-codes, swipe cards, biometric IDs, loyalty cards, customer passwords, etc.). While all mundane aspects of everyday life are moulded by surveillance practices this does not imply citizens are aware of this state of affairs. But although there may be no elaborate discourse about surveillance at this mundane level and the majority of citizens may not be aware of the fact they are being constantly surveilled, different ways of handling this status of being a person under surveillance can be observed and analysed. Citizens as techno-social hybrids have to handle issues of privacy, either by ignoring the problem, redefining what privacy entails and means or by taking some sort of remedial action to secure relevant elements of their private sphere. They have to find a way to use (or not use) new forms of electronic commerce, to manage their daily routines in the face of an encompassing surveillance regime, forcing them to identify themselves permanently, when engaged in institutionally mediated encounters, like e.g. in front of an ATM.

For an analysis of citizens' perspective towards surveillance and privacy, the following approach seems adequate to avoid problems of reactive methods (like explicitly asking for their attitudes towards surveillance) while at the same time learning something about what it means for a lay person to live in a surveillance society: Try to understand how different technologies (like mobile phones, loyalty cards, tablets, laptops) are used on a daily basis and what they are used for (shopping, communicating with friends, entering into exchange with public authorities, etc.). Having elicited a person's history of the multiple uses of different technologies the problem of surveillance, data protection and privacy can be addressed by asking for the respondents understanding of how these technologies work, what they are used for and what the effects of their daily use are, on the user. This produces a second, reflective level, demonstrating how individuals handle their existence as surveilled techno-social hybrids. WP 4 proceeded thus, by querying technology use, followed by user knowledge or concerns relating to the different uses.

The data of WP 4 shows that that individuals integrate surveillance related technologies (from mobile phones to swipe cards documenting their office hours) in many different, and often creative ways into their everyday lives. Daily routines are built around the uses of these technologies; they are perceived as means to facilitate daily business, open new opportunities, create new ways to communicate and socialise. The majority of the respondents had a positive attitude towards technologies, ignoring their potential for privacy intrusions and surveillance. Respondents were aware about the changes caused by new technologies in their lives, but typically perceived these changes as positive. Only a small fraction declared themselves as critical or reluctant technology users from the very beginning or reported taking precautionary measures (e.g. changing the default privacy settings in social media or using encryption). Before respondents were asked about their knowledge of the surveillance effects of the different technologies they were using, they were asked to provide their opinion about CCTV as one of the more popular forms of public surveillance. Most of the respondents had no clear understanding of the functioning of CCTV, but accepted this technology as a means to address problems of crime and vandalism, and as a technology enhancing public security.

Resilient reactions can be analysed by looking at the reflective parts of the interviews. When discussing the effects of the everyday use of technologies, a number of side effects were addressed in the interviews. We developed a typology of dilemmas to capture the varieties of

effects mentioned by the respondents. This idea builds upon the mainstream discourse of security, privacy and liberty. The implementation of new surveillance-based security measures is justified as a means to increase the level of security in the face of pertinent threats. These new measures often entail a loss of privacy and/or liberty. Such losses then are deemed acceptable, given the presumed increase of security levels. Playing on this logic of trade-offs, we constructed a number of dilemmas investigating how individuals handle surveillance in their daily lives.

Starting from the master frame of *security and surveillance* (which claims that greater surveillance increases security), we found a similar form of reasoning with regard to the levels of *convenience*: using technologies with high surveillance potential increases the level of convenience for a large variety of everyday activities (shopping, communicating, searching for information, travelling, etc.). Individuals leave data traces and once they start to reflect about their status as "leaking data containers", they begin to develop second thoughts about certain amenities: are the discounts offered for loyalty card holders worth the savings, when measured against the companies' strategy to create (individualised) consumer profiles? Is online shopping a viable alternative when the data created in the transaction might be used for targeted marketing strategies creating a constant flow of (spam) mails with unsolicited offers from companies, advertising their goods and services? Once individuals begin to reflect about these types of problems, resilient reactions start to emerge. Depending on the level of technological understanding (or computer literacy) individuals develop different strategies to avoid negative effects of their online behaviours, they begin to think about how they can fix some of the holes in their leaking data container, having second thoughts before they give away personal information.

Similar ideas about how to increase resilience to counter the effects of mundane surveillance were presented when addressing other dilemmas. When considering the privacy costs of social media platforms, individuals begin to understand that the idea of having a private space, when interacting with others via an electronic medium, is at least problematic. Resilient reactions can be observed when individual presentation of personal information on these platforms is given explicit consideration: what and how should I communicate on a social media platform? Once these questions become part of daily communicative practices, using the Internet, resilience builds up. What can be seen here in a typified way, is a trade-off between *privacy and sociality*. Respondents begin to understand that there are privacy costs associated with being an online person.

When addressing practices of surveillance in the context of electronic tools for surveillance applied in workplace environments, the emerging dilemma can be typified as a trade-off between *privacy and trust*. While in pre-electronic times employers tended to trust their employees (or had to trust them, since opportunities for intrusive surveillance were limited), with the introduction of workplace surveillance as a standard feature in many companies, trust has eroded. Workplace surveillance may have a positive effect, as some of the respondents pointed out, since controlling working hours can help identify free riders and "cheaters". On the other hand, being constantly monitored in a given environment tends to erode trust. Resilient strategies can take on different forms, depending on the type of surveillance practice and the overall context of the workplace situation. In some extreme cases, employees may quit their job as it is the only opportunity to escape constant surveillance. Other reactions involve legal actions against employers introducing surveillance systems or trying to work around or circumvent the installed systems.

One of the more prominent dilemmas, discussed in the literature on surveillance societies is the trade-off between *engagement and security*. Large-scale surveillance, particularly by state authorities can have (and does have) an impact on civic engagement and social protest. The fear that one's public activities are recorded, stored and could probably be used as evidence some time later, can have a chilling effect on citizens. This problem takes a reflexive (or even ironic) twist, when social protest targets surveillance as a practice of police and law enforcement authorities. Social activists have developed resilience measures such as hiding their faces when participating in public rallies. On the other hand, the same technologies that have a high potential for surveillance can be applied to organise new forms of social protest such as flash mobs. With regard to resilience in this domain the evidence seems mixed. While politically active individuals may experience the negative effects of surveillance more strongly and hence develop explicit resilient counter strategies, for the average layperson the spread of surveillance in public places may simply reinforce an attitude of political quietism, which often is the default state of most citizens. Nonetheless, resilience in this field has dramatic effects on the culture of social protest.

From the perspective of citizens, the average layperson shows limited awareness of surveillance as an abstract problem and hence resilience is rarely a categorical part of the repertoire of action. On the other hand, since surveillance prone technologies are part and parcel of everyday life, everybody has to develop a way to handle these technologies. Two findings seem to emerge from the research and in-depth interviews in WP 4. First, respondents, when confronted with the surveillance potential of their existence as techno-social hybrids, start to reflect about the dilemmas discussed above, weighing the loss of privacy that comes with surveillance technologies against the gains or losses of convenience, trust, civic engagement or security. Second, in those cases where citizens experience the (often unexpected) effects of surveillance, they begin to show resilient reactions of different kinds, depending on the type of technology involved and the individual capabilities to handle these technologies.

On the basis of the complex and highly differentiated views of citizens collected in WP4, we can conclude that different types of resilient reactions develop. There is one type of reaction that could be termed "surrender", i.e. citizens simply acknowledge the loss of their privacy that comes with the use of electronic media, and accept that life in contemporary societies is impossible without such technologies. These respondents embrace their status as techno-social hybrids without any efforts to maintain their privacy. Another form of reaction consists in different forms of coping. Here citizens use the – admittedly limited – opportunities to enhance their private sphere while being connected to the multiple surveillance-prone technological systems. This may help to create a feeling of empowerment although the effects in most cases are limited, given the state of the art e.g. in consumer surveillance for marketing purposes. A small number of respondents practised a form of resilient action which could be termed "resistance". They developed often highly creative strategies to actively disrupt surveillance practices. Though such strategies in most cases required a sound understanding of technological systems, not many of the respondents qualified as high-level experts in this field and so lacked the understanding and knowledge to exercise resistance. Finally, there is one strategy that was based on a cognitive strategy we termed "redefine and trust". Respondents in this category took up the interpretations and frameworks provided by the actors and institutions actively engaged in massive surveillance. Viewing the problem of surveillance and resilience from this perspective, all surveillance measures and data-collection practices appeared as reasonable and rational solutions to a problem. Whether this attitude qualifies as resilience in a literal sense may seem questionable. However, this is also a

reaction to massive changes in the very basic features of a society moving towards a new transparency, a reaction motivated by the desire to achieve or maintain a coherent self, even when there seems to be no answer, what this notion refers to, in a surveillance society.

5.1.3 Findings from WP5 – Exercising democratic rights under surveillance regimes

Dr Xavier L'Hoiry & Professor Clive Norris, University of Sheffield [964]

In the context of surveillance and democracy, the three principles of consent, subject access and accountability are at the heart of the relationship between the citizen and the information gatherers. The individual data subjects have the right to know what data is being collected about them and by whom, how it is being processed and to whom it is disclosed. Furthermore, they have rights to inspect the data, to ensure that it is accurate and to complain if they so wish to an independent supervisory authority who can investigate on their behalf.

Exercising one's right of access to personal data is a central feature of European data protection regulation. It is, arguably, the most important of the ARCO rights (access, rectification, cancellation, opposition) because, if one cannot discover what is held about oneself, it is not possible to exercise the remainder of these rights.

Our research found, however, that the spirit of the European Data Protection Directive has frequently been undermined as it has been transposed into national legal frameworks, and then further undermined by the evolving national case law. Citizens, in their role of data subjects, encounter a wide range of illegitimate restrictions in their attempts to exercise their rights. These restrictions are enacted through a series of discourses of denial practiced by data controllers or their representatives.

The WP 5 research was conducted in three parts. The first part involved a comparative analysis of European and national legal frameworks in the area of data protection and, specifically, subject access rights. In the second part, researchers undertook empirical work – attempted to locate data controllers, their contact information and key content regarding data protection and subject access rights. In the third part (also empirical), researchers with submitted subject access requests, in relation to their own personal data, to a range of data controllers to assess this process and the responses received from these organisations. As such, the WP 5 deliverable is made up of country reports written by researchers in the ten participating institutions. These country reports will offer in-depth analyses of exercising informational rights in country-specific contexts.

[964] The following partners were involved in the research and the data presented here is the result of their fieldwork: Professor Clive Norris (University of Sheffield, UK); Dr Xavier L'Hoiry (University of Sheffield, UK); Antonella Galetta (Vrije Universitiet Brussel, Belgium); Professor Paul de Hert (Vrije Universitiet Brussel, Belgium); Dr Ivan Szekely (Eotvos Karoly Institute, Hungary); Beatrix Vissy (Eotvos Karoly Institute, Hungary); Dr Rocco Bellanova (Peace Research Institute Oslo, Norway); Professor J. Peter Burgess (Peace Research Institute Oslo, Norway); Maral Mirshahi (Peace Research Institute Oslo, Norway); Stine Bergensen (Peace Research Institute Oslo, Norway); Marit Moe-Pryce (Peace Research Institute Oslo, Norway); Jaro Sterbik-Lamina (Institute of Technology Assessment, Austria); Stefan Birngruber (Institute of Technology Assessment, Austria); Dr Chiara Fonio (Universita Cattolica del Sacro Cuore, Italy); Alessia Ceresa (Universita Cattolica del Sacro Cuore, Italy); Professor Marco Lombardi (Universita Cattolica del Sacro Cuore, Italy); Dr Gemma Galdon Clavell (Universitat de Barcelona); Liliana Arroyo Moliner (Universitat de Barcelona); Dr Erik Lastic (Univerzita Komenskeho v Bratislave, Slovakia); Roger von Laufenberg (Institut fur Rechts und Krimialsoziologie, Austria); Professor Nils Zurawski (Universitat Hamburg, Germany)

Legal frameworks

Data subjects are inherently disadvantaged even before they can begin the process of submitting a subject access request. This is in part because the implementation of the EU Data Protection Directive 95/46/EC has been uneven across EU Member States and, in the development of case law, many European countries have interpreted key provisions of the European law in a narrow way. As a consequence, European citizens living in different countries are subject to very different regimes in relation to:

- legally defined response time in relation to obligations of data controllers;
- requirements upon data controllers to appoint Data Protection Officers;
- the costs of making a subject access request;
- the complaints and redress mechanisms available to data subjects with their national Data Protection Authorities.

This means that, not only are there considerable differences at the European level, but that an access request emanating from one country, but submitted to another, may be subject to completely different procedures. This inconsistency is particularly true of provisions related to the concept of 'motivated requests', (Belgium and Luxembourg) which demand that data subjects legitimise their requests with a justified reason accompanying the submission of the request itself. In such cases, it seems that exercising one's rights as set out in the European Data Directive is not a justified reason in and by itself, and often leaves the data subject at the mercy of the data controller's discretion to determine what constitutes a legitimate reason.

Locating the data controller

The right of access is exercised by submitting an access request to a given data controller but, before this can begin, one must locate the data controller. This phase of the empirical work was conducted as follows:

- The research was conducted across 10 European countries[965] and examined 327 individual sites in which personal data was routinely collected and stored.
- The research sites were chosen based on a consideration of the socio-economic domains in which citizens encounter surveillance on a systematic basis. These domains were health, transport, employment, education, finance, leisure, communication, consumerism, civic engagement, and security and criminal justice.
- Researchers attempted to locate data controllers and their contact details in a variety of ways including by telephoning them, visiting sites personally and accessing organisations' online content.

The research sought to determine the ease and/or difficulty of locating data controllers, given the centrality of this process as the natural pre-condition of citizens being able to exercise informational self-determination.

The research found that, in a significant minority (20%) of cases, it was simply not possible to locate a data controller. This immediately restricts citizens' ability to exercise their right of access due to the insufficiency of information regarding who one should send access requests

[965] The research was carried out in the following countries: Austria, Belgium, Germany, Hungary, Italy, Luxemburg, Norway, Slovakia, Spain and the UK.

to. Where data controllers could be located, the quality of information concerning the process of making an access request varies enormously from country to country and in different sectors, both public and private. In the best cases, information was thorough and followed legislative guidelines closely, providing citizens with an unambiguous pathway to exercise their right of access. In the worst cases, information was very basic, often failing to explain how to make an access request or indeed what an access request actually is. Information was often confusing and incomplete, consequently obliging the citizen to pro-actively seek clarifications before being in a position to submit a request.

The most reliable, efficient and frequently used way of locating data controllers turned out to be online. In nearly two thirds (63%) of all cases, online searching provided the relevant contact details, and this was achieved in less than five minutes over half (61%) of the time. Attempts to locate data controllers using alternative methods generally did not fare well. In the majority of cases, when contacting organisations by telephone, members of staff lacked knowledge and expertise concerning subject access requests. As a result, answers were often incorrect, confusing and contradictory to the organisations' own stated policies.

When it was possible to locate the data controller via telephone, this took over 6 minutes, sometimes on premium rate lines, in over half (54%) of all cases. Even then, the quality of information provided via telephone was rated as 'good' in only 34% of cases.

In the case of CCTV, where researchers personally attended the sites:

- nearly 1 in 5 sites (18%) did not display any CCTV signage;
- where signage was present, in over four out of ten cases (43%) it was 'poor' in terms of its visibility and content;
- only one third (32.5%) of CCTV signage identified the CCTV system operator or the data controller.

By failing to display appropriate signage at CCTV sites, one fifth of organisations effectively employed 'illegal' practices. The expertise of members of staff when approached in person was found lacking and they frequently reacted to queries with suspicion and scepticism, questioning why one would wish to access their personal data. Thus, even where researchers were merely trying to find the contact details of the data controller, they were forced to justify why they sought to exercise their democratic rights, and even then they were frequently denied.

Submitting access requests

When it is possible to locate the data controller, the process of then submitting an access request can be problematic as data controllers employ a range of discourses of denial which restrict or completely deny data subjects the ability to exercise their informational rights.

- Subject access requests were sent in 10 European countries to 184 individual organisations sampled from the first part of the empirical phase of the research.
- This sample set included both public and private sector organisations as well as a number of key multinational organisations which routinely collect large amounts of data.
- The requests were made for a range of data, including information held on paper and digital records and CCTV footage.

- Requests made three key demands of data controllers: disclosure of personal data; disclosure of third parties with whom data had been shared and disclosure of whether (and if so how) data had been subject to automated decision making processes.

The research found that obtaining a satisfactory response concerning all aspects of the requests was a relatively rare occurrence.

- Four out-of ten requests (43%) did not result in personal data being disclosed or data subjects receiving a legitimate reason for the failure to disclose their personal data.
- In over half of all cases (56%), no adequate or legally compliant response was received concerning third party data sharing.
- In over two-thirds of cases (71%) automated decision making processes were either not addressed or not addressed in a legally compliant manner.

Even taking account of those cases in which successful outcomes were achieved, the process of submitting an access request was often fraught, confusing and time-consuming.

- Holding/acknowledgment letters were received in only a third (34%) of cases, which meant that data subjects had no idea whether the requests were being dealt with or simply ignored.
- Even where data subjects received information about their personal data, the disclosure was incomplete and additional data was still outstanding. This occurred in one third of cases (31%) and required researchers to pursue data controllers for more information as the first disclosure was incomplete.

There were noted variations in how different types of organisations responded to requests. In general, public sector organisations performed less badly than those in the private sector, with only 43% engaging in restrictive practices compared with 62% in the private sector. Requests for CCTV footage were particularly problematic, with seven out of ten requests for CCTV footage facing restrictive practices by data controllers or their representative. While loyalty card scheme operators were generally facilitative in disclosing personal data (86% of cases), they did not perform as strongly in providing information about automated decision making processes (only 50% of cases). Meanwhile, requests to banks did not yield much information about third party data sharing (only 30% of responses disclosed this).

In assessing both the process of submitting access requests as well as the content of the responses received from data controllers, the research found a range of restrictive practices employed.

- Data controllers frequently render themselves 'invisible' to data subjects using a variety of practices, ranging from the absence of CCTV signage identifying who is operating the cameras to flatly refusing to respond to access requests at all. In 12 cases, requests were met with complete silence. In a further 17 cases, although preliminary communications were entered into, subsequent correspondence elicited no response. Ultimately, in total, therefore, one in six cases (15%) of all cases was met with silence.
- Many organisations did not have clear and formal administrative procedures in place to receive and respond to subject access requests. These bureaucratic failures led to considerable delays and confusion for data subjects in the manner that their requests were processed. This included the inability (or unwillingness) of data controllers to

respond to requests in any language other than English despite receiving requests in other language.

- Data controllers often responded to requests only after long and excessive delays. This at times had a direct impact on the availability of the data requested (e.g. the deletion of CCTV footage). It also meant that data controllers were in breach of their legal obligations to respond to requests within nationally specified time frames.
- Some data controllers, particularly multinational corporations, offered only fixed and pre-determined mechanisms for data subjects to submit requests. These mechanisms did not allow for specific queries to be addressed and took an extremely narrow and, in the context of European law, invalid interpretation of the type of data citizens are entitled to request.
- In many cases, data controllers refused to fulfil requests by invoking legal provisions incorrectly. This showed a lack of knowledge and expertise on behalf of data controllers and their representatives as data subjects were erroneously advised that they had no legal entitlement to exercise their rights.

Achieving a successful outcome when submitting an access request is possible and researchers came across a significant minority of cases, for instance in Germany and the UK, where requests were dealt with courtesy, diligence and efficiency. However, the burden of achieving a successful outcome lies heavily with the data subject and many of the organisations targeted in this research did little to lift this burden away from the citizen: members of staff repeatedly reacted with surprise and bewilderment to requests, explaining that they had never received such queries before. A vicious circle therefore emerges, where organisations fail to inform citizens of their rights or how to exercise them. As a result, for those citizens who have little or no prior knowledge about privacy and data protection issues, the right of access is either unknown, denied or inaccessible. Due to the lack of subject access related queries received from the public, organisations fail to inform/train their staff in matters of privacy and data protection, and have little motivation to do so.

The empirical results of the research demonstrated significant disparities in the ways requests were processed from one country to another. The research shows that this is partly due to the willingness of data protection authorities in some countries to support citizens when they exercise their informational rights. This, coupled with the absence of the need for data subjects to provide a justified motivation for their requests, meant that submitting such requests was generally a smooth process in these countries. In contrast, in Italy and Spain, the researchers encountered a plethora of restrictive practices ranging from the identification of data controllers, the ways in which their requests were processed, and the difficulty of submitting complaints to DPAs when disputes arose.

The results of the research have led to a wide number of broad and general policy recommendations. Some of the key points to emerge are:

- Data controllers should take steps to render themselves more ‘visible’ and simplify the access request process for data subjects by implementing recognised procedures to process access requests.
- Data controllers should provide data subjects with clear and intelligible information about the personal data they process and how data access requests may be made.
- There should be no motivation required when submitting an access request other than the wish to exercise one’s democratic rights, notably the right to protect personal data.

- If data controllers invoke legal exemptions when refusing an access request, they should specify the exemptions relied upon.
- Data protection authorities should provide templates and guidance for data subjects and data controllers to use when citizens seek to exercise their informational rights.
- Data protection authorities should also provide an unambiguous and free redress mechanism for data subjects to complain.
- Civil society organisations should be encouraged to promote access and other informational rights.

The myriad restrictive practices evidenced in this research means that data subjects have to work extremely hard to exercise their rights. They have to show persistence, confidence and resilience in the face of a series of discourses of denial during which their access requests may be regarded as illegitimate, severely delayed or simply ignored altogether. Even then, they are only likely to successfully exercise their rights fifty-percent of the time.

Policy implications and recommendations

In light of the experiences outlined above, we outline a number of policy implications and recommendations aimed at the practical level at both data controllers and DPAs, and at a more theoretical level at the legal frameworks surrounding the exercise of informational rights by data subjects.

Legal

The research found that the intentions of European legislation on data protection and privacy are sometimes undermined by the implementation of these laws into national legislative frameworks. Through national legislation itself, or in the development of case law, citizens' ability to exercise their informational rights are often hampered, providing data controllers with exemptions from their obligations to disclose personal data and restricting data subjects in their attempts to improve their understanding of how and what personal data is processed. Moreover, there is a fundamental absence of harmonisation of both administrative and bureaucratic processes and the resources provided to bodies such as DPAs, from one Member State to another. As a result, we propose:

- The concept of 'motivated requests' in national legislation should not be used – exercising one's democratic rights should be considered as sufficient motivation.
- Data controllers should show a legitimate legal reason for denial of requests. In other words, the burden of proof should be on data controllers to show that a request should be denied rather than the burden of proof being on data subjects to legitimise their requests.
- The form and content of CCTV signage should not be left to the discretion of the operators but should be legally regulated i.e., signage should be standardised in terms of size and the information contained within.

Data controllers

Some data controllers demonstrated high levels of facilitative practices during the research and these instances demonstrated that best practices can be achieved across different sectors and in the context of requesting different types of data. However, other data controllers frequently employed a wide range of restrictive practices, policies and procedures which,

deliberately or otherwise, prevented citizens from exercising their access rights. Amongst many others, such restrictive practices included administrative and bureaucratic failures, rigid and pre-determined processes which did not encourage specific queries and perhaps worst of all, outright silence. As a result, we propose the following:

- Data controllers should make themselves as 'visible' as possible. The relevant office/department/individual to whom access requests must be sent should be easily identifiable, and a full contact address provided. This would give citizens a clear indication of the data controller.
- Data controllers should have a designated individual or department with the responsibility for receiving and processing access requests. This does *not* mean that all data controllers should employ a dedicated Data Protection Officer to deal exclusively with data protection matters. Rather, this may simply be an existing member of staff with other duties and responsibilities who has received sufficient training to enable them to process and respond to requests in a legally compliant manner.
- When disclosing to data subjects with whom their data is shared, it should not be sufficient to simply list categories of recipients. Such practices undermine data subjects' ability to exercise their informational rights. Instead, data controllers should specifically list the third parties with whom personal data is shared and their contact details.
- When disclosing information about automated decision making processes, data controllers should provide clear and complete information about how these processes work, the logic underpinning these processes and the effect they have on the decisions made about the data subject.
- When data controllers use their online privacy policies to disclose content about their data protection and privacy practices, these policies should include a section on access rights indicating the following:
    - A statement that data subjects have the right of access
    - A reference to the relevant legislation
    - A description of how to submit an access request including an outline of what to include in a request
    - An outline of identification requirements as part of submitting an access request
    - Contact details for the individual/department who processes requests
    - Privacy policies should always outline what type of data the data controller collects, processes, for what purposes it is collected, with whom it is shared (see above) and whether it is subject to profiling (and if so, how).
- Telephone numbers given as the contact for privacy queries (e.g. on CCTV signage) should not lead to a generic call centre. Instead, they should be directed to a member of staff with requisite expertise to answer questions on privacy. Alternatively, the data controller should ensure that members of staff answering these telephone calls receive sufficient training to recognise a data protection query and escalate/pass such queries appropriately to a relevant officer or department. Ideally, this process should never involve more than two people.
- Telephone numbers for data controllers should not involve premium phone charges as this essentially represents an additional tax on citizens in exercising their democratic rights.

- Members of staff should be sufficiently trained to either answer privacy-related question themselves or have a clear protocol to escalate such queries to a relevant management figure. Ideally, this process should involve no more than two people.
- Data controllers should consider providing data subjects with templates to make their requests. This will ensure that requests are easily recognised and that all the required information is included in a single correspondence.[966]
- Language should be given serious consideration by data controllers in responding to subject access requests. Ideally, responses to access requests should be made in the requester's own language. However, while it may not always be possible to respond to data subjects in their own language, it should not simply be assumed that the requester can speak English.
- Data controllers should show flexibility in their processes when receiving access requests. For instance, the use of email as an acceptable format via which to submit requests should be encouraged, especially in cases when the data controllers themselves are inherently digitally-based (i.e.: social network organisations).
- Data controllers should carefully consider the manner and format in which they disclose personal data in order to ensure the intelligibility of the data. This is especially important for those data controllers who process large amounts of data held in big data sets.
- In the case of CCTV images, the rights of third parties should not be used to thwart access requests. Data controllers should be required to develop policies and proceedures to enable this.[967]

Data Protection Authorities

The research revealed an endemic lack of awareness of informational rights and specifically access rights amongst both data subjects and data controllers. The absence of knowledge amongst data subjects that they have the right to request copies of their personal data means that this right is rarely exercised and few requests are submitted to data controllers. In turn, given the scarcity of such requests, many data controller representatives do not receive any training on how to process and respond to such queries in a legally compliant manner. The results of this vicious circle are that data controllers frequently display inadequate practices and procedures when faced with access requests, and data subjects lack the awareness to recognise such poor practices and challenge them to achieve a satisfactory outcome.

When poor practices are challenged, the first recourse is usually the DPAs. However, the research also showed that in some cases, DPAs' resources (or lack thereof) are such that they are unable to process complaints in a satisfactory manner and this can therefore become a lengthy process. As a result, we recommend:

- DPAs should prioritise the promotion of informational rights to citizens and consider how training/awareness-raising could be delivered.

[966] See for example the template provided by Interpol available at http://www.interpol.int/About-INTERPOL/Structure-and-governance/CCF/Access-to-INTERPOL%27s-files. This is a simple and short template but ensures that all necessary details are included in order to process the access request in a timely and efficient manner.

[967] For instance, data controllers should make use of footage blurring technology if they possess this. If this is not available, data subjects may, for instance, be invited to inspect the footage even if they cannot be given a copy of it.

- DPAs should provide standard model templates for data subjects to use in order to submit an access request.
- DPAs should, in conjunction relevant stake holders such as consumer rights and labour organisations, promote the development and acceptance of standard templates in specific sectoral contexts.
- DPAs should provide detailed guidance to data controllers on how to respond to access requests including examples of best practice[968] and consider how specific training could be delivered.[969]
- DPAs should also provide detailed guidance to data subjects on how to exercise their rights.
- DPAs should ensure that a clear, unambiguous and affordable complaints procedure is available to data subjects in case of data breaches.
- DPAs should have the power of audit and inspection; this would go some way to redress the asymmetry of power between data subjects and data controllers.
- DPAs should proactively audit public and private sector organisation websites and other channels of communciation to see whether all relevant information is available to citizens to make a sucessful access request.

Post-script: policy recommendations in light of the European reform

The policy implications and recommendations resulting from our research findings are made on the basis of the existing European and national legislation. The EU is currently in the process of reforming Directive 95/46/EC and some comments can be made here in the light of our research findings which address the substance of the proposed reforms.

First, our research found considerable variation in how subject access rights are enacted in different Member States. The use of a Regulation rather than a Directive would lead to greater consistency between different countries.

Second, the research demonstrated that the presence of DPOs facilitated the access request procedure for the data subject. Any proposal which seeks to diminish organisations' responsibilities to appoint DPOs needs to consider the detrimental effect that this may have on citizens' abilities to exercise their rights.

Third, our research illustrated that privacy policies often lacked the requisite depth of detail to enable data subjects to manage their data in a meaningful way. If citizens are to be empowered to exercise their rights, organisations must clearly describe their subject access procedures and policies, and provide explicit protocols to submit an access request.

Fourth, the research found that data controllers were generally reluctant to disclose any information about their data sharing protocols and even when pushed, only revealed generic lists of who they shared personal data with. While this is in accordance with the current legislation, it is quite clearly inadequate as data subjects are completely in the dark about whom personal data is actually shared, how it is then used and processed.

[968] See for example the Information Commissioner's Office (2012) 'Draft Subject Access Code of Conduct' http://www.ico.gov.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/draft_subject_access_cop_for_consultation.ashx

[969] See for example the courses provided by Amberhawk in the UK – http://www.amberhawk.com/training.asp

Fifth, our research showed the almost complete inability of data controllers to address when and how automated decision making processes were used. As such, proposals which demand that data controllers properly address issues of automated decision making and profiling should help alleviate this problem.

Sixth, our research showed that the obligation to justify and motivate requests acted as an unwarranted restriction on data subjects' ability to exercise their rights. This should be explicitly addressed in the proposed reforms.

Finally, as our research has clearly illustrated, in the case of transnational corporations, there is a lack of clarity as to which national legislation they are subject to and whether they are subject to European legislation at all. This appears to be an area that legislators need to urgently address.

6 CONCLUSIONS

6.1 COMPARISON BETWEEN THE EMPIRICAL AND THEORETICAL FINDINGS

This section presents some comparisons between the empirical findings of WPS 3-5 listed in section 5 and the review of resilience theory and state of the art outlined in sections 2.2 (horizontal analysis of the domains), 3.4 (horizontal analysis of the case studies) and the section 4 focussing on resilience in a surveillance society.

As shown before, WP3 of IRISS involved three case studies representing different types of surveillance: ANPR, Credit Scoring and Neighbourhood Watch. The three case studies were examined in different European countries. One of the central findings was that increasing resilience to surveillance in Europe begins with increased public and institutional awareness of its harms and its benefits. As shown in the theoretical analysis, both awareness and communication are important elements of resilience. It is important to have strategies and policies to address both these aspects. Awareness raising and communication of information should occur on an ongoing basis to sustain resilience.

The theoretical analysis particularly demonstrated in the case of resilience in [dictatorial and] post-dictatorial regimes that historical and other factors are relevant and often determine the nature of societal resilience. Though the intersection between surveillance and democracy across the three case studies in WP3 varied, patterns emerged associated with historical, legal, political, social and institutional factors. To a greater degree than ever before, surveillance processes intersect with and constitute the way in which we get things done. The case studies underscore the need to question how transparency and accountability re-organise themselves in surveillance societies; this will enable alternatives to emerge (noting that transparency and accountability are both critical to resilience as shown in the study of resilience in the banking sector and some of the adverse events such as the NSA revelations).

WP3 showed that ANPR resulted in some harms against which resilient strategies need to be formulated. Credit scoring pointed to a problem with transparency, and with the operation of the rule of law. Controversies associated with credit scoring were evident in all of the case study countries, but in some cases the media have been slow to react, resulting in ill-informed consumers and unaccountable, non-transparent banks. The NW case study showed how the presence of NW-like organisations could stigmatise particular spaces and focus on victimising those perceived as the 'other' at that moment. Whilst it is inevitably difficult to prioritise

resource deployment in the current public financial climate, it is important for the police (and consequently other public agencies) to be connected with the communities they serve. These points illustrate some of the complexities at play in surveillance societies that resilience strategies will have to take into account.

WP4 focused on citizens' attitudes towards surveillance practices as an element of their everyday lives. This WP shows that concepts such as "surveillance", "privacy", or "resilience" are not common coinage for most European citizens most of the time, except for situations where problems of surveillance score high on the political and media agenda. As demonstrated in the theoretical analysis (domains and adverse events) in this report, WP4 shows that resilient strategies can take on different forms, depending on the type of surveillance practice and the overall context of the situation. There are also differential effects of surveillance on stakeholders - while politically active individuals may experience the negative effects of surveillance more strongly and hence develop explicit resilient counter strategies, for the average layperson the spread of surveillance in public places may simply reinforce an attitude of political quietism, this being the default state of most citizens. Nonetheless, resilience in this field has dramatic effects on the culture of social protest.

The complex and highly differentiated views of citizens collected in WP4 illustrate different types of resilient reactions – e.g. "surrender", where citizens simply acknowledge the loss of their privacy; "coping" where citizens use the – admittedly limited – opportunities to enhance their private sphere while being connected to the multiple surveillance prone technological systems; "resistance" where they develop highly creative strategies to actively disturb surveillance practices; and "redefine and trust" where they take up the interpretations and frameworks provided by the actors and institutions actively engaged in massive surveillance. In contrast, the theoretical analysis of the different domains revealed a greater variety of (and sometimes overlapping) aspects of resilience: to withstand, to survive, to adapt, to quickly recover, sustain status quo, harness local resources and expertise, to rally stakeholders together, to manage, to transform, to bounce back (and even forward). The resilience strategies evident via WP4 seem more limited than these, or rather are not yet fully developed in the form of these many, different permutations.

WP5 which focussed on exercising democratic rights under surveillance regimes. It undertook a comparative analysis of European and national legal frameworks in data protection and, specifically, subject access rights, found, that the spirit of the European Data Protection Directive has frequently been undermined as it has been transposed into national legal frameworks, and then further undermined by evolving national case law. Citizens, as data subjects, encounter a wide range of illegitimate restrictions in their attempts to exercise their rights. The myriad restrictive practices mean that data subjects have to work extremely hard to exercise their rights. Data subjects have to show persistence, confidence and resilience in the face of a series of discourses of denial during which their access requests may be regarded as illegitimate, severely delayed or simply ignored altogether. While this WP calls for greater resilience for data subjects, we need to recognise that resilience might not be the only need of the hour. Further, resilience is best supported by a multi-pronged approach where the relevant stakeholders (data subjects, data protection authorities, private companies, the public sector) are rallied to achieve its purpose.

6.2 FINDINGS AND RECOMMENDATIONS

Resilience in the domains

Examination of resilience in different domains shows that the term resilience is often widely used and defined in different ways, and that its conceptualisations often share similarities and differences. Some of these conceptualisations have proved useful, while others not so much, in the context of this project. The domains analysis revealed a number of things about resilience. Resilience is multifaceted; sometimes it has an opportunistic aspect. It has a temporal as well as a spatial aspect. It involves communications between stakeholders. It calls for solidarity. Its core elements include: anticipation of vulnerabilities, threats, attacks, crises; preparedness; prevention, detection and response; mitigation; recovery and the sharing of responsibility and co-operation among stakeholders. Resilience also suggests a coherent set of objectives and measures aimed at achieving them in the face of typical human and natural threats to national security and community disruption. The key learning from the domains analysis was that the framing of resilience measures can often benefit from lessons learned from prior events with the aim of mitigating future adverse events. However, resilience measures do not always anticipate very well their own sometimes negative and counter-productive consequences.

Measures that could contribute to a more robust resilience strategy to make systems, individuals, groups and society resilient include:

- Policy dialogue
- Good risk management and sound risk methodologies and vulnerability assessment
- Standardisation
- Increased transparency
- Regional and/or international approaches to resilience rather than only a national approach
- Multi-stakeholder approach
- Stakeholder collaboration and co-ordination
- Flexibility
- Innovation
- Learning lessons from past or concurrent experience elsewhere

Some key features or elements of a resilience strategy against surveillance derived from our analysis of resilience in different domains:

- The ability to identify and mitigate specific challenges of surveillance;
- An examination of the different social aspects as well as how surveillance takes place in different sectors of our economy;
- The acknowledgement of the complexity of systems and the high reliance of societal activities on them;
- The acknowledgment of the impossibility of ensuring maximal security, and the need to accept risk(s), and to eschew the trade-off paradigm where security is balanced against privacy or other fundamental rights;
- The need to foresee and prepare against aggressive instances of surveillance;
- The need to rally different and new actors, sharing responsibilities, knowledge and resources with them;

- The institutionalisation of the latent strengths, in order to be able to calculate them in foresight exercises, and to nurture and train stakeholders; and
- Effective, structured communication.

Resilience in the adverse events

The examination of the adverse events provides the following insights:

- Resilience measures can often learn from prior events and aim to mitigate future adverse events.
- While resilience can be improved through planning and exercises organised by central authorities, it can spring unmolested from wellsprings that some people don't even know they possess.
- Resilience can be strengthened by reviewing what happened during past adverse events.
- The obvious risk with additional surveillance and new legislation (as reactions to adverse events) is that the pendulum will swing too far towards improved security and, in the process, create new risks to privacy and other fundamental rights.

The adverse events also underline the following:

- The need for a more proactive and efficient approach to regulate privatised surveillance and its effects.
- The need to inculcate and develop a culture of vigilance to surveillance, particularly in relation to the design and implementation of new technologies. This vigilance is a multi-dimensional construct, needing to be developed by each stakeholder and across stakeholders.
- Better co-ordination, sharing of information and learning of lessons between relevant authorities across the EU.
- Need for greater accountability, particularly on the part of industrial actors designing and implementing cutting edge surveillance solutions without adequate investment in examining effects or monitoring threats from those solutions that affect or have the potential to affect human rights and fundamental freedoms.

The open nature of democracy: resilience and vulnerability

In a democratic society people are free to act and live their lives as they wish, singly or in groups, as long as they do so within laws that are not arbitrary and with tolerance and respect for the rights of others to do so. It is also a society in which people have wide latitude to develop their autonomous personalities, to pursue their interests and projects, and to form social relationships to the maximum degree consistent with the possibility for others to do likewise, and not to have to seek permission from 'authority' to engage in these self-developmental activities. Democratic societies can be as vulnerable to attacks on their open nature, as are democratic political systems. The freedoms and rights enjoyed by the infrastructures, groups and individuals of a democratic society might be restricted or undermined by similar kinds of threats, as those that interfere with the workings of politics and government. Ostensibly protecting democratic freedoms and rights, resilience measures – perhaps especially those that involve *surveillance* – might themselves lead to a more closed society that brings democracy into question. If we take the public sphere as a property of

democracy, we can understand how (state) surveillance poses a threat to its functioning and integrity.

Resilience in a surveillance society

This report defines resilience as the *ability of people (individuals and groups) and organisations to adapt to and/or resist surveillance, while recognising that some forms of surveillance may be acceptable or tolerable, while others pose a serious challenge to our fundamental rights.* Resilience in the context of surveillance is different from resilience in the instance of the capacity of an infrastructure or of a community disrupted by an earthquake, tsunami or a financial calamity. Although it may come as a shock or a revelation to some people when they realise how extensive and pervasive surveillance has become, much of the surveillance today can be regarded as an ongoing stress on society, rather than a shock. Hence, resilience in a surveillance society has more to do with coping than with recovering or bouncing back. Further, in a surveillance society, there is clearly a difference between resisting surveillance and adapting to it. It is possible to resist surveillance, but resistance may not prevent surveillance. One might also see resilience as on a continuum somewhere between surrender and civil disobedience.

Measures to increase resilience in a surveillance society

This deliverable outlines various measures to increase resilience in surveillance societies amongst which are political and regulatory measures (such as accountability and oversight, explicit consent, privacy principles, creating boundaries and limiting surveillance, awareness and communication), individual measures (such as whistle-blowing, resistance and using privacy-enhancing technologies), and societal measures (such as public opinion polls and an activist press). The list is not exhaustive. As surveillance continues to grow and expand, such measures need to be reinforced and strengthened at all levels. Individuals and societies need to take active and sustained measures to curtail surveillance and its dangerous and deleterious effects.