



risk & regulation is also published on **carr**'s website:
www.lse.ac.uk/CARR
www.lse.ac.uk/riskandregulationmagazine

risk & regulation: **carr** review
No 32 Winter 2016

Editors
Martin Lodge and Andrea Mennicken

Published By
Centre for Analysis of Risk and Regulation,
London School of Economics and Political
Science, Houghton Street, London WC2A
2AE, UK

Enquiries
Centre Administrator, Centre for Analysis
of Risk and Regulation, London School of
Economics and Political Science, Houghton
Street, London WC2A 2AE, UK.

Email: risk@lse.ac.uk
Telephone: +44 (0) 20 7955 6577
Fax: +44 (0)20 7955 7420

www.lse.ac.uk/carr

Copyright in editorial matter and this
collection as a whole: London School of
Economics © 2016

Copyright on individual articles:

p. 03 © Martin Lodge, Andrea Mennicken
p. 06 © Martin Lodge, Andrea Mennicken
p. 08 © Robert Rizzi, Charles E. Borden
p. 12 © Lavinia Cadar, Maureen Donnelley
p. 14 © Jeremy Brice
p. 16 © Hanan Haber, Eva Heims
p. 18 © Filippo Cavassini, Faisal Naru,
Bill Below
p. 21 © Martin Lodge
p. 24 © Michael Power

All rights reserved. No part of this publica-
tion may be reproduced, stored in a retrieval
system, or transmitted, in any form or by
any means, without the prior permission in
writing of the publisher, nor be issued to the
public or circulated in any form of binding or
cover other than that in which it is published.

The School seeks to ensure that people
are treated equitably, regardless of age,
disability, race, nationality, ethnic or national
origin, gender, religion, sexual orientation or
personal circumstances.

Design and Art Direction
Harald Müller

Printed By
Hobbs the Printers Ltd

Cover image
Adobe Stock: Steve Gerig

Photography and Illustrations
Adobe Stock: raphaelbrunk, cristovao31,
xixinxing, patronestaff, VolkOFF-ZS-BP,
Tatyana Gladskih, sukvijit, MStock (3),
teerawit, bpstocks

ISSN 1473-6004
Online ISSN: 1473-6012



contents

Editorial Martin Lodge and Andrea Mennicken	03
Regulating security Martin Lodge and Andrea Mennicken consider the growing currency of security in risk and regulation debates	06
Security clearances and the regulation of national and domestic security personnel Robert Rizzi and Charles E. Borden advocate changes to existing approaches	08
Building transboundary crisis management capacities in Europe Lavinia Cadar and Maureen Donnelley point to the critical tasks at the core of transboundary crisis management	12
Blissful Ignorance? Risk management and knowledge of food supply chains Jeremy Brice considers whether management of risk through strategic ignorance is past its sell-by-date	14
Regulating for and with the masses: A new era of regulation? Hanan Haber and Eva Heims discuss the growing significance of regulation for social and distributive purposes	16
Are regulators the new Men in Black? Not when it comes to independence ... Filippo Cavassini, Faisal Naru and Bill Below call for a fresh look at regulatory independence	18
Regulating in the dark: oversight over intelligence services Martin Lodge considers the relationship between transparency and security	21
The artefacts of risk management Michael Power highlights the effortful nature of risk management practice	24
carr news	26
carr people	28

editorial

Security is the theme of this latest issue of risk®ulation – a theme that has featured extensively in **carr**'s activities over the past six months, and which also raises important questions that are shaping our future research agenda.

The topic of security has received less attention in risk and regulation scholarship than the theme of safety. We suggest that it is time to devote more attention to security and the relationship between safety and security. Amongst other things, security is about the identification of threats and the definition of what is worth preserving. Both such undertakings are highly political ones, as is the devising of strategies to promote security. How to provide security to citizens when exposed to potential transboundary threats from large-scale infrastructure failures has been a growing theme as there has been a growing awareness of potential vulnerabilities. Equally, debates about the appropriate regulation of the security state have received heightened attention. Such debates are of a long-standing nature. However, events such as 9/11 and information-technological changes have arguably changed the nature of the debate around security. One such change can be seen in the rise and amalgamating of the notions of 'homeland security' and 'societal security' which have brought together the civil protection and intelligence arms of the state. Concerns with the activities of intelligence services and cyber security have given rise to debates about appropriate regulatory oversight. These debates are reflected in the contributions by Robert Rizzi and Charles Borden and by Lodge in this issue.

Security touches on many other themes central to **carr**'s research activities, whether relating to questions of food security and transboundary crisis management, or to the management of indicator and other quantified steering systems.

Security is necessary to provide space for life to flourish, notwithstanding questions and concerns about its ambivalence. Also, the intellectual life of **carr** can only flourish in somewhat secure surroundings, both in an institutional and financial sense. Funding from the European Union's Horizon 2020 scheme and the Open Research Area initiative that brings together different national research councils – in the UK, the ESRC – form a cornerstone of that security. The Horizon 2020 TransCrisis and ORA QUAD projects are now up and running and harvesting their first findings, as illustrated by the contribution by Lavinia Cadar and Maureen Donnelly. Alex Griffiths has joined us as a research officer on the QUAD project. More recently, we have been successful in bringing together funding from the Food Standards Agency and LSE's knowledge exchange and impact fund for a co-funded research officer position. Jeremy Brice, who we have appointed to this position, introduces in this issue his earlier work on food security. Finally, we managed to secure funding from the UK Prosperity Fund for a study (together with RAND Europe and the Brazilian IPEA) to investigate the regulation of logistics infrastructures in Brazil.

Funding is certainly an important prerequisite for good research and **carr** depends on it. Yet, that on its own would not be sufficient. For **carr** to provide a venue for cutting-edge interdisciplinary research in risk and regulation support is needed from institutions that accept explorations at the overlapping peripheries of different social science disciplines. In an age where disciplines and deans often seek to assert particularistic core understandings by pressing for publications in the 'top three' journals, the provision of such a secure space cannot be taken for granted. We are grateful to LSE's Department of Accounting for granting such space in both a physical and an intellectual sense.

carr has always understood its role to be a venue to bring together perspectives from the worlds of research and practice. A few months ago, **carr** brought together international researchers from law, political science and history to explore whether regulation scholarship is in crisis (see also the contribution by Haber and Heims in this issue). This event illustrated the central place that **carr** can play in bringing together and advancing international debates and collaborations. That event took place a few days before the Brexit referendum. Whatever shape Brexit might take, Brexit represents an existential threat to UK higher education in general and **carr** in particular. In that sense, the world has certainly become less secure for international research collaboration, although, ironically, Brexit has placed debates about transnational regulatory standards and their enforcement even more prominently on the policy agenda.

Whatever the outcome of the Brexit process, we are committed to continuing **carr**'s role in the international conversation on risk and regulation, and we are greatly looking forward to your comments and contributions. **Martin Lodge & Andrea Mennicken**



Regulating Security

Martin Lodge and **Andrea Mennicken** consider the growing currency of security in risk and regulation debates

Security is not a term that has enjoyed widespread currency in the field of risk and regulation. Most attention has traditionally been paid to questions of 'safety': how to ensure the mitigation of harm by controlling for deviating operating practices (such as allowing poorly maintained ships into harbours). Less attention has been paid to security: the mitigation of external threats (such as provisions for harbour screening systems). Such concerns have conventionally featured in the field of international relations.

Why, then, consider security in the context of risk and regulation? There are a number of reasons why security has become increasingly prominent in fields of study that have customarily been more interested in safety. For one, increased attention has been paid to the vulnerabilities of large critical infrastructures across countries – leading to the adoption of national risk assessment and management plans. Further, there have been changes in the field of civil protection and contingencies. The divide between the 'security state' of intelligence agencies, the police and the military, on the one side, and the 'civil protection' state, on the other, has become increasingly blurred, especially after 9/11, as evidenced by the creation of the Department of Homeland Security in the US. Similarly, the increased concern with 'societal security' has brought together agencies from the different 'security' and 'protection' fields.

To some extent, this blurring responds to changing perceptions of threat: cold-war era concerns with aerial bombardment have been supplanted by fears about attacks on critical infrastructures. The weekly siren drills to ensure that populations could be warned about an impending attack have vanished. Of course, the newness of such concerns should not be overplayed; states have been concerned with the security of energy (oil), water and food reserves to deal with potential disruptions for a long time. Similarly, announcements that individuals should stock sufficient

water and food supplies to maintain a certain degree of self-sufficiency, at least for short periods, are also nothing new, especially in areas prone to natural disasters.

However, there have also been some notable changes. Ideas about security have become more prominent and widespread. In the area of finance, reforms have sought to ringfence activities so as to make markets more secure from contagion. Ideas of food security have been revisited in the context of international production chains. Furthermore, the justification for civil protection has altered. There has been an increasing formalization of crisis infrastructures across European public administrations at all levels of government. There have also been changes in justification, for example, the German federal government's announcement of its new civil protection plan in the summer of 2016 stressed that the threat was not related to traditional warfare but stemmed, instead, from threats to critical infrastructures posed by cyber-security related attacks.

The importance of algorithms, online communication and energy infrastructures in everyday life has been widely discussed. These raise important questions for risk regulation, if alone in the context of scenario building exercises. For example, the modern classic 'Black-out' by Marc Elsberg was used as a reference point by the German Federal Minister of the Interior to justify the issuing of a new civil protection plan. In that novel, the sustained hacking into computer networks quickly destroys social and economic infrastructures across European states and the US. The awareness of growing vulnerabilities due to cyber attacks has also been noted in the context of attacks on national communications systems, voter databases, and nuclear reactors.

However, security issues do not just relate to questions of collective welfare and the protection of critical infrastructures. Algorithms are deployed by private and public organizations to

predict individual and organizational behaviours and preferences on the basis of collected data. Much of these data are collected in non-transparent ways (for example, via smartphones and other electronic devices). Generally, individuals casually consent to becoming 'quantified selves' in order to access 'convenient' online services.

The security implications of such a trend are at least twofold. The first concerns the security of the systems that gather data. These include worries with regard to the security of individuals about whom information exists that they themselves might not be aware of. Individuals are also unlikely to understand the algorithms that are being applied to target specific messages to them, whether these are links to advertisements, selected news outlets or other messages. There are also questions about the transparency and accountability of the algorithms themselves which, in turn, raises much wider issues about how to regulate artificial intelligence. Such issues become ever more problematic from a viewpoint of risk and regulation when data collection is used for granting access to public services, or to allow organizations to make discriminatory choices, such as differentiated pricing regimes in health insurance.

The security of the individual – in terms of protecting their right to privacy – often collides with broader, societal or governmental security considerations. Such concerns have given rise to various regulatory regimes dealing with phone-tapping and other extraordinary powers to invade an individual's private sphere. How such regimes are developed, how they are being held to account and with what consequences, are issues that have not enjoyed much currency in the wider risk and regulation literature.

The second major security implication relates to the security of the organizations gathering and utilizing information. The security of organizations' collected data is regularly questioned in view of high profile hacking or da-

ta-breaching incidents. Apart from concerns about firms' cyber security provisions, and suspicions about the motives of such hacking incidents, debates about how to develop regulatory standards in such a transboundary context remain largely under the surface.

This gives also rise to questions pertaining to the regulation of data-sharing across organizations. Under what conditions, for example, should private organizations be required to provide data to public organizations, if the latter claim to be acting on behalf of societal security? Indeed, as debates around Edward Snowden (and others) have shown, the public exposure of highly intrusive and extensive activities of intelligence services is seen by some as worthy whistleblowing to alarm the public about 'dangerous' activities of certain state organizations. For others, such whistleblowing activities represent attacks on the security of the state and its citizens (if not 'treason'). Others, in turn, might question whether standards are being applied to private and public organizations when it comes to data collection. Certainly, there is some qualitative difference in the case of state-based organizations that have the power to utilize information to restrict liberty directly. Nevertheless, in the case of private organizations, regulation might need to be applied against the interests of individuals and firms in order to 'defend' constitutional norms of privacy and the 'right

to forget' and to restrict data exchange between different applications. Such questions become ever more pertinent as certain online services become utility-like facilities – without access to such services, individuals are unable to fully integrate into social and economic life. In other words, the world of non-state cyber-security has reached a degree of publicness that calls for the development of regulatory regimes to protect individuals.

Harold Laswell in his classic 'The garrison state' of 1941 painted a picture of a future in which specialists of violence had replaced the specialists of bargaining (business). A modern-day Laswell (as arguably depicted in David Egger's *The Circle*) would most likely put his emphasis on data science specialists who enjoy considerable power through their knowledge, their capacity to identify individual preferences and lifestyles, and their ability

to deliver tailored messages to bespoke publics. In our contemporary world, critical questions therefore relate to the balance between individual and societal security and how national and regional organizations can seek to regulate such transboundary activities. This is not to say that all national power to regulate has vanished, as can be seen by the particular security arrangements regarding the data protection applicable to EU-funded proposals.

But security-related questions should also be more generally at the centre of debates about risk and regulation. Security assumes the existence of a threat. This threat is directed at a certain state of the world that is seen as desirable. The identification of threats (or 'the other') is a highly political process as is the definition of desirable states of the world deemed worth protecting. This raises questions as to what or who is being threatened, such as individuals or collectives. It also questions about 'who' is causing a threat, whether these are state or non-state, national or international organizations or individuals. Regulating security links to a world in which emergency powers exist and where private organizations are tied closely to state powers in order to allow for the continued functioning of critical infrastructures. It links to questions as to how much security an individual should be granted in view of potentially opposing interests by the security state. This hidden world that seeks to provide security requires more interrogation. The tensions that emerge in the regulation of security go to the heart of constitutional democracy. They are therefore of fundamental relevance to the study and practice of risk and regulation.

Martin Lodge is Director and **Andrea Mennicken** is Deputy Director of **carr**.



Security clearances and the regulation of national and domestic security personnel

Robert Rizzi and **Charles E. Borden** advocate changes to existing approaches

In recent years, Western security establishments have been subject to a number of significant security breakdowns, with individuals obtaining and widely disseminating massive amounts of classified information. These breakdowns have highlighted some of the limits of the current security process, both in terms of how information is classified, and the process by which governments determine who may have access to classified information.

In the US, and elsewhere, the core component of the process by which a person is provided access to certain categories of classified information is the 'security clearance'. Initially developed during the second world war, and greatly expanded in the early years of the Cold War, the security clearance process rests on a 'certification model' – at prescribed points in time, an assessment is made of an individual's suitability to receive classified information, and the individual is either 'certified' and receives clearance or is denied. The process focuses on the government's national security interest with little weight given to the individual's personal interest – the ability of an applicant to appeal a denial of a security clearance is fairly limited. This approach, however, has begun to show strains, as the changing nature of both government and information has created new challenges for which the current security clearance system is not optimally designed.

In particular, the expansion in the size of government and the increasing use of private contractors in national security-related activities, coupled with rapid changes in information and communications technology, has resulted in a clearance process that is both too broad and insufficiently reliable. The number of government and government-related positions that require security clearances has exploded over the past couple of decades, despite questions about whether and to what extent many of these positions are

likely to encounter classified information. This explosion in the number of security clearances that need to be processed has in turn stretched the resources of those agencies responsible for administering the security clearance regime. At the same time, the computer and communications revolution has expanded the volume of classified information exponentially during the same period, making the consequences of a security breach potentially far more wide-reaching than they were in the past. Put simply, under the current security clearance process, significant resources have to be expended on certifying security clearances for individuals and positions that pose little security risk, and at the same time the risks associated with a potential breach have increased substantially.

Moreover, security clearances have taken on a regulatory role that extends well beyond their original purpose of protecting sensitive information. In effect, the security clearance assessment has become less an inquiry into whether a person is capable of handling specific types of sensitive information and more a determination of whether a person should be allowed to work in government or government-related professions. As a practical matter, the failure to obtain a security clearance can end or significantly damage a person's career, and therefore the individual economic stakes for applicants are substantial. Yet, the present security clearance process provides individuals with little ability to challenge a negative security clearance determination.

A changing landscape

Although the security clearance process has broadly remained unchanged since the 1950s, the landscape in which it operates has changed significantly. The growth in the size of the US government, coupled with an increased tendency to designate positions as requiring a security clearance even where there is little likelihood

that they will encounter classified information, has led to a massive increase in the number of security clearance reviews that are performed every year. Indeed, it is estimated that in 2014, 5.1 million individuals, primarily Americans, had security clearances granted by the US government (Fung 2014), including roughly 1.5 million at the Top Secret level, and that the cost of 'vetting' those individuals was approximately \$6 billion (ibid). Moreover, attachment of a security clearance to a particular individual increasingly has become a form of government franchise or licence. This licence determines whether or not the individual can serve in a wide range of government positions, as well as in private sector positions that have quasi-governmental functions, regardless of whether the position will require contact with classified information (Rizzi et al., 2015: 24-27). This trend has made a security clearance, especially at the higher levels such as Top Secret, a 'bankable' qualification, and a requirement for working in a large number of fields that may be only tangentially related to national security.

Challenges

The current system has created a one-way ratchet in terms of requiring clearances, and of the corresponding scope of clearance investigations. The result has been delays in performing background checks and the use of third-party contractors to conduct investigations, with a predictable impact on quality. Comprehensive monitoring of individuals with access to classified information is limited, and in some spectacular cases, has proved to be inadequate.

Because a security clearance is required for a range of positions, a denial or revocation of a clearance constitutes a de facto regulatory bar to public service. The American system has developed an elaborate process of implementing denials and revocations of security clearances, using terminol-





ogy borrowed from the legal sphere. For example, security clearance denials for private contractors are 'adjudicated' before 'administrative judges' as part of 'hearings and appeals'. But, in fact, the current review system in many respects bears only a superficial resemblance to due process. As the scale of the security clearance process has expanded, and as the holding of a clearance has increasingly become a prerequisite for government jobs and contracts, there has not been a commensurate increase in the protections afforded to individuals in connection with granting or revoking their clearances. Indeed, the rights of affected individuals with respect to clearance determinations have, if anything, been reduced as a result of deferential judicial doctrines.

A major structural flaw in the current security clearance system is its reliance upon a certification model. Under the original 1953 regulatory scheme, as slightly modernized in the 1995 Executive Order, the scheme depends almost entirely upon standardized procedures to determine whether an individual can be 'cleared' for access to classified information and, if answered in the affirmative, the clearance certifies the individual can have such access going forward, even though neither the government nor the individual knows precisely what information will be involved in the future. Moreover, certification systems generally operate on a 'snapshot' in time, often failing to take into account changes in the certified person or his or her circumstances over time.

As with any certification system, the current approach purports to provide assurance, and to create a presumption of continued validity, once the certificate is issued. Many of the spectacular examples of failures of the system involve individuals who may have at one point been deemed sufficiently trustworthy, but became dangerously unreliable, as the result of a variety of changing factors, such as financial distress.

Risk-based reforms?

One possible approach to reforming the current security clearance system would be to rely upon a risk-based personnel evaluation system, which would emphasize ongoing compliance and monitoring, rather than a single certification. A risk-based approach would provide a more comprehensive set of categories of individuals with contact with classified information to replace the three basic categories now used. Such an approach would concentrate resources on those positions as to which individuals would be most likely to handle, or be exposed to, classified information, particularly classified information that creates significant national security risk, and would focus on comprehensively mitigating that risk. In practice, this approach would mean reversing the one-way ratchet, with fewer positions requiring any form of clearance, and with those positions requiring clearance being risk-weighted at the outset. In implementing this approach, it should be possible to measure actual and probable contact between the individual's position and classified information, and to apply more rigorous standards to those with greater access. For example, an individual acting as a systems administrator or maintenance worker with broad access to classified information through highly sensitive IT systems would be subject to the most rigorous standards, regardless of title or seniority. The risk assessment thus would be based on current and probable future activities of the individual, rather than seniority of position.

Furthermore, a reformed compliance and monitoring model could modify or replace a half-century old certification system. Especially for positions that have access to particularly sensitive information, frequent and random reporting and responses to selected inquiries (for example, questions concerning unusual changes in financial holdings or transactions) could provide deterrence from inappropriate

conduct with respect to such information. Similar models have been developed in the past to address analogous conduct risks, for example, testing regimes for restricted substances and drugs (for recipients of government licences and airline pilots), and for monitoring potential financial conflicts of interest. These regimes also tend to create and reinforce norms of conduct that reinforce the regulatory regime, because of the periodic reminders that the individual is subject to a special set of rules.

References

- Cabinet Office (2013) 'Government security classifications, April 2014.' London: Cabinet Office. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf> Accessed day, month, year.
- Fung, B. (2014) '5.1 million Americans have security clearances', *Washington Post*, 24 March 2014. <<https://www.washingtonpost.com/news/the-switch/wp/2014/03/24/5-1-million-americans-have-security-clearances-thats-more-than-the-entire-population-of-norway/>> Accessed 27 October 2016.
- National Counterintelligence and Security Center (2015) '2015 Annual Report on Security Clearance Determinations.' Washington DC: Office of the Director of National Intelligence. <<http://www.fas.org/sgp/othergov/intel/clear-2015.pdf>> Accessed 27 October 2016.
- Rizzi, R., Borden, C. and Holman, D. (2015) 'Ethics regulation of government contractors.' *risk®ulation* (winter): 24-7. <<http://www.lse.ac.uk/accounting/CARR/publications/CARRmagRR30-PDF-Version.pdf>>
- Robert Rizzi** is partner at Steptoe & Johnson LLP and **Charles Borden** is partner at Allen & Overy and a **carr** visiting fellow.

Building transboundary crisis management capacities in Europe

Lavinia Cadar and Maureen Donnelley point to the critical tasks at the core of transboundary crisis management

The world of crisis is changing. The refugee crisis, the Eurozone crisis, Brexit or terrorism – the modern crisis cannot be tamed unilaterally. These transboundary crises cut through geographic, political, policy, cultural, economic or legal domains. They require transboundary crisis management capacities.

The European Union (EU) must adapt to this new world of crisis if it is to demonstrate continuing relevance in the face of ever-growing threats. The EU has in place modest capacities to help member states manage crises within its boundaries and beyond. But the EU can do more, we argue, to assist member states. In thinking about potential trajectories for institutional design, it is helpful to think of crisis management as a set of tasks that have to be fulfilled in each and every crisis: detection, sense-making (understanding what is going on), making critical decisions, coordinating a response network, communicating about the crisis, and rendering account for the

response actions (Boin et al., 2016).

These tasks are particularly hard to implement in a transboundary context. Here is what the EU may try to accomplish.

Detecting an emerging crisis may seem straightforward. But in many cases, critical bits of information must be pieced together and deemed relevant by a considerable number of people before a crisis is recognized. The EU has in place a large number of early warning networks that gather information on the origin, spread and severity of many threats. Yet, early signs of a transboundary crisis must make their way through the complicated and time-consuming process of national and EU agenda-setting, where they become subject to consensus-forming among member states. The trajectory of early warning signals must be streamlined.

Once an emerging crisis has been detected, it is crucial to understand what is going on. Identifying sources, collecting information, analysing ambiguous and often conflicting data. **Sense-making** is not easy in the bordered world of national states and agencies. When the number of actors involved stretches across geographical borders, when the crisis management authorities are not hierarchically related, when it is uncertain who knows what and where information must come from and go to, sense-making is a daunting task. During the 2010 Icelandic volcanic ash crisis, none of the EU member states dared to reopen air traffic as uncertainty loomed over the composition, size and direction of the ash cloud, as well as the ash tolerance limits of jet engines. In the early phases of the global financial crisis, the division of competencies between the EU and member states on monetary and economic policies made it difficult to understand what exactly was happening and which institution needed to do what.

The EU has various crisis centres and is working to put procedures in place that will help to process information, share it across boundaries and understand information from other sectors and/or countries, thus facilitating a shared response. But many barriers



remain, especially when it comes to sensitive intelligence.

The biggest problem in a transboundary crisis is the absence of clearly demarcated **decision making** powers. While the US has at least addressed this problem through its National Response Framework (NRF), the EU is still stuck with the decision making structures that were designed to deal with complex but not urgent problems.

Think of the refugee crisis. The large numbers of people from Syria and elsewhere arriving at Europe's borders highlighted serious limitations of the EU's joint decision making process. Initially, humanitarian concerns dominated responses. However, other issues, such as those relating to security, health and wider economic impacts, soon emerged. These concerns had to be weighed against a background of conflicting and incomparable information on the number, identity and

affiliation of the refugees, as well as political pressures, budget restrictions, education and social services limitations, and divided sentiments among host communities. The lack of an appropriate decision making process to quickly bring together the many jurisdic-

tions involved resulted in paralysis. Uncertainty over who (EU institutions, national leaders and authorities such as health services or border control, international organizations) should deliberate, and how, made it impossible to enable a comprehensive course of actions that could reduce the impact of the crisis.

Even when all national leaders agree on a course of action, the efforts of member states must be **coordinated** somehow. After all, the EU (like NATO) has no resources of its own. The EU's agencies have very little coordinating power.

After the outbreak of the avian influenza (H5N1) in 2005, the European Commission made efforts to coordinate member states in abiding by the WHO's recommendation regarding antiviral stocks. However, these efforts stranded in debates over the centralization of antiviral stockpiles, in criti-

cism from pharmaceutical companies on member states' delays in approving vaccine manufacturing, and in controversy over some member states' decision to vaccinate birds (Boin et al., 2013).

In the face of a transboundary crisis, it is critical that leaders **communicate** effectively and do so from the same song sheet. The recent terrorist attacks in France, Belgium and Germany were followed by different interpretations over causes and what must be done to contain them. Conveying a shared message that remains true to the espoused values of the EU turned out to be a challenging task for European leaders. This challenge will no doubt become increasingly relevant in the face of simplistic explanations and extremist solutions put forward by populist politicians across Europe.

Finally, successful crisis management concludes when the actors **render account** about decisions and strategies initiated before, during and after the crisis, as well as the rationale behind those decisions. When it is not clear who owns a crisis and who is responsible for what, particularly when multiple actors across borders are involved in responding to a transboundary crisis (think of the refugee crisis), a clear process of accountability is hard to imagine. The lack of accountability deepens the EU's democratic deficit. The European Parliament should push for improved procedures to hold EU leaders accountable for their (non-) involvement in managing transboundary crises.

Preparing individual institutions to respond to crises is no longer sufficient. Effective transboundary crisis management hinges on fostering successful cooperation across a far wider response network. Management demands amplify greatly when a crisis not only requires scaling up an institution's hierarchical chain, but

also pervades multiple policy domains, jurisdictions and systems, requiring coordinated efforts among multiple organizations (Ansell et al., 2010). The EU has limited capacities to facilitate the effectuation of the crisis management tasks set out above. But it can do more. We suggest three possible initiatives:

- › Define a European vision on transboundary crisis management. This manifesto should set out what the EU can do to help member states, along the lines of the NRF in the US.
- › Integrate the various institutional capacities now found in separate policy domains under one EU roof.
- › Refine training and preparation efforts rather than investing in large-scale exercises, pursue trainings that facilitate the effective implementation of detection, sense-making, decision making, coordination, communication, and accountability.

References

- Ansell, C., Boin, A. and Keller, A. (2010) 'Managing transboundary crises: identifying the building blocks of an effective response system'. *Journal of Contingencies and Crisis Management* 18(4): 195–207.
- Boin, A., Ekengren, M. and Rhinard, M. (2013) *The European Union as crisis manager: patterns and prospects*. Cambridge: Cambridge University Press.
- Boin, A., 't Hart, P., Stern, E. and Sundelius, B. (2016) *The politics of crisis management: public leadership under pressure*. 2nd edn. Cambridge: Cambridge University Press.

Lavinia Cadar is a junior consultant at Crisisplan and works primarily on the TransCrisis project. Maureen Donnelley is a consultant at Crisisplan.



The TransCrisis project (full name: Enhancing the EU's Transboundary Crisis Management Capacities: Strategies for Multi-Level Leadership) is a three-year project funded by the European Union under the Horizon2020 programme. carr is the co-ordination partner in this network of eight organizations. Other partners involve: Crisisplan (Arjen Boin), the University of Utrecht (Femke van Esch), Central European University (Nick Sitter), Institut Barcelona d'Estudis Internacionals (IBEI, Jacint Jordana), University of Catania (Fluvio Attina), University of Stockholm (Mark Rhinard) and ThinkTank Europa (Maja Rasmussen). More information can be found at the project website www.transcrisis.eu.

Blissful Ignorance? Risk management and knowledge of food supply chains

Jeremy Brice considers whether management of risk through strategic ignorance is past its sell-by-date

In November 2013 the Food Standards Agency and the Economic and Social Research Council announced a £1.87 million research programme focusing on food safety, food fraud and consumer trust within the UK agri-food system. Operating under the auspices of the UK Global Food Security Programme, this initiative called Understanding the Challenges of the Food System, would explore public perceptions of food supply chains and analyse the resilience, integrity and security of those supply chains. These had, the programme's funders explained, become issues of major public concern and urgent policy relevance following the discovery earlier that year that processed meat products ranging from burgers to lasagne and meatballs had been adulterated with horsemeat.

Academics and food regulators were not alone in experiencing pressure to deliver improved knowledge of food supply chains in the aftermath of the events that became known colloquially as 'Horsegate'. As Peter Jackson has observed, Horsegate tended to be characterized within prevailing narratives as a product of systemic deficiencies in the governance and control of international food supply chains, rather than as the result of malpractice within individual food businesses, or of shortcomings in national regulatory regimes. For instance, the Elliott Review (2013: 18) into the Integrity and Assurance of Food Supply Networks – the most totemic of the official inquiries sparked by Horsegate – suggested that much of the UK food industry's vulnerability to fraud stemmed from the complexity of its supply chains and commented that:

'The first part of risk management is to know who you are doing business with. The food industry could do well to ... improve the knowledge and grip on all parts of the supply chain. ... Understanding your supply chain, and how it works, must be much more than maintaining an appropriate paper trail.'

By this account, Horsegate was a pathology of opaque and convoluted global supply chains which extended far beyond the regulatory reach of any single enterprise or nation state and included numerous layers of murky and unaccountable intermediaries. As such, it appeared that more detailed knowledge of long and complex food supply chains would be required if the risk of food fraud was to be controlled and future adulteration scandals averted.

As a researcher attached to a project funded under the Understanding the Challenges of the Food System programme, I have been an attentive observer of post-Horsegate efforts to achieve an improved

knowledge of the workings of food supply chains and to understand their attendant risks. The project on which I worked – 'Making provisions: anticipating food emergencies and assembling the food system' – examined how actors involved in the production, processing, retail and governance of food go about anticipating potential emergencies and crises before they occur, and how they develop plans to prevent, pre-empt or manage such events. Over the past two years, my colleagues and I have closely followed the rapid proliferation of technologies and services (including specialist audits, brand protection services and supply chain mapping techniques) designed to help food businesses to identify and control potential risks within their supply chains.

We found ample evidence of interest in these services within food businesses. Supply chain managers

and technical staff spoke eagerly of mapping supply chains spanning continents and embracing hundreds of companies, and of utilizing supply chain data to developing new risk analysis techniques. Yet in practice many food businesses' knowledge of and influence over their supply chains extended only as far as the companies from which they bought their products or ingredients. While these immediate suppliers were typically subjected to



painstaking programmes of audit and analytical testing, few food businesses considered themselves responsible for ensuring that risks were managed and compliance was maintained throughout their extended supply chains. Monitoring the companies supplying their suppliers – and the suppliers serving those companies in turn – was, we were told repeatedly, 'the supplier's due diligence'.

The relative inattention of many food businesses to their wider food supply chains appears to be a (possibly unintended) effect of the manner in which criminal penalties for breaches of food law are currently apportioned within the UK regulatory regime. Under due diligence provisions within British food legislation, persons and organizations cannot be held liable for food safety or authenticity offences committed by their associates if they can prove that they took all reason-

able precautions to prevent such an incident from occurring. As a result, a food business's liability for cases of contamination, fraud or food-borne disease often hinges on the question of whether it could reasonably have foreseen that the actions of companies within its supply chains might result in a breach of food law. A food business which had access to, or was in a position to obtain, information indicating that such a breach was likely

to occur within its supply chain would find itself exposed to costly and reputationally damaging litigation. Meanwhile, one which could not reasonably have been expected to obtain such information would not be held legally to be responsible.

This means that investing in identifying the companies which make up their extended supply chains, or in gathering information about the emerging risks and threats to which those companies might be exposed, may not always be in food businesses' best interests. While possession of this information might indeed help a business to prevent breaches of food law and thus avert potential crises, it might also be taken as evidence that its staff could have foreseen offences committed by companies within their supply chains. In short, food businesses are presently caught between a hope that improved knowledge of their supply chains might help them to better manage the risk of food scares and scandals, and an awareness that possession of such knowledge could place them at risk of prosecution for offences that they did not commit.

Caught in this double bind, many British food businesses appear to be

managing their own exposure to supply chain risk through what Linsey McGoeys might term a policy of 'strategic ignorance'. For McGoeys (2012: 559), strategic ignorance is a name for practices which ensure that: 'unsettling knowledge is thwarted from emerging in the first place, making it difficult to hold individuals legally liable for knowledge they can claim to have never possessed'. In this case, food businesses limit their liability for breaches of food law through ensuring that their knowledge of their extended supply chain remains sufficiently limited that they may plausibly claim that they could not reasonably have foreseen any incidents which might occur within it. Many such businesses appear to have concluded that this can best be achieved by working hard to demonstrate that their immediate suppliers are responsible companies which can reasonably be trusted to ensure that compliance is maintained among the businesses which make up their extended supply chain.

This cultivation of a strategic ignorance of the threats and vulnerabilities which may exist within extended supply chains arguably plays as crucial a role in the risk management strategies of many food businesses as does the production of knowledge about those supply chains. Yet many participants in the Making Provisions project also felt that this ability to maintain a strategic ignorance of their supply chains might itself be increasingly a risk. In the aftermath of the Horsegate scandal key food industry assurance schemes such as the British Retail Consortium's Global Standard for Food Safety were overhauled, and now place greater emphasis on the traceability of food-stuffs and on the assessment and management of food fraud risk at all levels of the supply chain. Meanwhile the Modern Slavery Act, passed in 2015, obliged businesses with an annual turnover of more than £36 million to publish an annual statement detailing

what steps they have taken to ensure that all parts of their supply chain are free of human trafficking, slavery, servitude and forced labour.

Such developments suggest that both legislation and private sector regulatory arrangements may be moving gradually towards a position that ignorance of lapses with one's extended supply chain is no defence – a trend which raises questions for academics and risk management practitioners alike. Even if risk management approaches which mobilize a strategic ignorance of supply chains remain legal, are they still acceptable either to food regulators or to the general public? What might be the impact upon the food industry of any potential move towards a regulatory model premised upon a complete knowledge of, and tighter control over, food supply chains which are global in scale and enormous in scope? And if the management of risk through strategic ignorance is to become a thing of the past, then just how is risk to be regulated and governed within the food supply chains of the future? Perhaps those currently grappling with such questions might be forgiven for concluding that ignorance was indeed bliss.

References

Elliott Review. (2013) 'Elliott Review into the integrity and assurance of food supply networks – interim report.' London: HM Government.

Jackson, P. (2015) *Anxious Appetites: food and consumer culture*. London: Bloomsbury Academic.

McGoey, L. (2012) 'The logic of strategic ignorance'. *British Journal of Sociology* 63(3): 553–76.

Jeremy Brice joined **carr** as a Research Officer in October 2016. He was formerly a postdoctoral Research Associate at Newcastle University, where he worked with Dr Andrew Donaldson and Dr Jane Midgley as part of the Making Provisions research team.

Regulating *for* and *with* the masses: a new era of regulation?

Hanan Haber and **Eva Heims** discuss the growing significance of regulation for social and distributive purposes

In 2015, the Well-being of Future Generations (Wales) Act 2015 was enacted, aimed at 'improving the social, economic, environmental and cultural well-being of Wales' (Welsh Government, 2015a). The Act requires public bodies to 'think long term', involve the public and those affected by policy and ambitiously 'take action to try and stop problems getting worse - or even stop them happening in the first place' (Welsh Government, 2015b). A cheerful animated video commissioned by the government follows the future life trajectory of a new-born, Megan (Welsh Government, 2015c), depicting how the Act will enable her to have a fulfilling and secure future, in employment, health, culture and environmental terms.

What explains this legislation in the first place? Why legislate for this cause, and why involve citizens in its implementation? Although adorable, animated babies do not lobby for legislation, nor do they organize in interest groups, vote or make political contributions. While it may be fairly intuitive to explain policy which overlooks individuals, causes or groups with little political clout, the growth of regulation aiming at protecting and involving those with little political voice (such as future generations or the economically vulnerable) comes as a surprise to regulatory scholarship and those who take a cynical view of political and regulatory processes.

We argue this Act is part of two wider trends, worth exploring together. The first is the growth of regulation for social and distributive purposes, and the second, the

growth of 'regulatory participation', involving citizens directly in regulatory decision making. This means regulation for social and redistributive purposes is growing in scope and significance. This is specifically so referring to vulnerable citizens, increasingly shielded from the market in different national settings and across sectors, from the regulation of the disconnection due to non-payment in the utilities, to 'mortgage rescue' schemes in housing credit, to regulating fees in pension markets, with wide variation between sectors and national settings (Haber, 2011, 2015, 2016).

In the second trend, we can also increasingly observe the emergence of 'participatory regulation', in which formerly expert-dominated regulatory decision making now entails citizen involvement. Examples range from policing to environmental regulation, demonstrating citizens' increasing involvement in governance processes at the local level by deliberating, rather than voting, about how government policy or services affect them, in different ways. Even in two jurisdictions of the UK, England and Wales, and Scotland, we have seen different types of participation emerge in the same sector at the same time, namely in price-setting in water regulation (Heims and Lodge, 2016).

These developments may signal a tentative move away from a regulatory world that is predominantly shaped by the concern to reassure investors.

Interestingly, increased participation is often accompanied by a stronger representation of vulnerable or 'voiceless' citizens in regulatory processes. For example, despite the mentioned different nature of customer engagement in water regulation in Scotland as opposed to England and Wales, customer representatives in both jurisdictions were able to push water companies to be more mindful of their most vulnerable customers (especially large families on low incomes) during the last price review.

Regulating for the voiceless, regulatory participation and legitimacy

A simple explanation for both

trends in regulatory policymaking might be that a rise of participatory regulation and representation of the vulnerable in regulatory processes may be aimed at alleviating concerns about the legitimacy of regulatory processes. Given that legitimacy of expert-led non-majoritarian regulatory bodies has long been questioned, we may assume that participatory approaches and representation of the vulnerable can remedy the 'legitimacy deficit'.

Whether this is indeed the case, however, crucially depends on what we think regulatory objectives ought to be and how they can be achieved. Is regulation about long term stability in the market or is it about meeting the (short or long term) interests or needs of different groups of citizens? At the very least, more representation of

interests is not only a pluralist dream but also means important trade-offs between very different kinds of goals, all of which we can safely assume to be societal values. While more participation may provide the appearance of more legitimacy, it may also increase controversy regarding what is perceived as legitimate regulatory decisions.

The shifting of political, social and environmental decision making to the regulatory arena, while also changing how regulatory decision making operates, signifies interesting times for citizens and scholars of regulation alike. As regulatory objectives as well as the nature of regulatory processes are in flux, it remains unclear how new tensions arising from this ongoing shift are to be reconciled and what consequences this transformation will have. In order to gain a better understanding of these issues, scholars and practitioners of regulation thus need to seek to understand what is driving these processes, how tensions between different goals are to be reconciled, and who speaks for those with and without a voice.

References

Haber, H. (2011) 'Regulating-for-welfare: a comparative study of "regulatory welfare regimes" in the Israeli, British, and Swedish electricity sectors'. *Law & Policy* 33(1): 116-48.

Haber, H. (2015) 'Regulation as social policy: home evictions and repossession in the UK and Sweden'. *Public Administration* 93(3): 806-21.

Haber, H. (2016) 'Rise of the regulatory welfare state? Social regulation in utilities in Israel' *Social Policy & Administration*, doi/10.1111/spol.12194/pdf.

Heims, E. and Lodge, M. (2016) 'Innovation through customer engagement and negotiated settlements in water regulation: towards a transformed regulatory state?' **carr** Discussion Paper no. 83. London: London School of Economics and Political Science.

Welsh Government (2015a) 'Well-being of future generations (Wales) Act 2015.' <<http://gov.wales/docs/dsjlg/publications/150623-guide-to-the-fg-act-en.pdf>> Accessed 27 October 2016.

Welsh Government (2015b) 'Well-being of future generations (Wales) Act 2015.' <<http://gov.wales/topics/people-and-communities/people/future-generations-act/?lang=en>> Accessed 27 October 2016.

Welsh Government (2015c) 'Video - Well-being of future generations (Wales) Act 2015.' <<http://gov.wales/topics/people-and-communities/people/future-generations-act/future-generations-act-video/?lang=en>> Accessed 27 October 2016.

Hanan Haber is LSE Fellow in the Department of Government. **Eva Heims** is Lecturer in Public Policy at the University of York. Both are **carr** Research Associates.

Are regulators the new *Men in Black*? Not when it comes to independence ...

Filippo Cavassini, Faisal Naru and Bill Below call

for a fresh look at regulatory independence

The *Men in Black* are a special unit charged with *regulating* Alien activity on planet Earth (at least it is in the film with Will Smith and Tommy Lee Jones). Their job is to operate incognito, working behind the scenes to avoid an intergalactic apocalypse. When uncovered, special technology allows them to eradicate all knowledge of themselves and their function.

To most of us, regulators are a lot like the *Men in Black*, ensuring that trains will run on time, that there is clean water in the tap, that lights switch on, that the broadband is working and that there is cash in the ATM machines. They largely go unnoticed, that is, until something goes wrong, stops working or crashes.

Unlike the *Men in Black*, regulatory agencies do not operate incognito – or they shouldn't. They must be part of a well functioning and transparent governance eco-system that provides these important public services and are held accountable for the performance of their different actors. Being part of this eco-system, however, carries a number of risks.

Different stakeholders – whether regulated industry, government, politicians, consumers or other interest groups – have powerful incentives to influence or capture regulatory policies. The danger of capture is all the more present be-

cause of the proximity of regulator and the regulated.

We need regulators to be independent, just as we need our judges and referees to be independent. However, independence cannot come at the price of accountability or engagement, and regulators need to keep their fingers on the pulse of the market through interaction with industry and consumers. In addition, autonomy should still be compatible with maintaining helpful feedback loops between the regulator and its governmental executive overseers. In a nutshell, regulators must be engaged but not enmeshed, insulated but not insular.

Given the challenging context within which regulators operate, the question is how to limit undue influence in practice and create a strong culture of independence. In the quest for an answer, the OECD first set out to understand how regulatory agencies around the world are structured to be protected from undue influence. The OECD has developed a unique dataset of the formal arrangements for independence of regulators across 33 OECD countries, complemented by detailed *case studies* showing what holds regulators accountable for their performance.

The dataset does not capture cases where regulators conform to established practices but are not legally bound to do so

through a formal or codified requirement. For example, a number of regulators publish forward-looking action plans although they are not required to do so by law. In essence, the dataset reflects the *de jure* situation in OECD countries in relation to the levels of independence, accountability and scope of action in six network sectors. In terms of independence, it shows that Germany and Italy have the highest measures for *de jure* independence (Koske et al., 2016).

The OECD (2016) has conducted a follow-up study in its recently published *Being an Independent Regulator*, which has filled in many of the gaps in our understanding of how *de facto* independence plays out in the daily life of regulators. Forty-eight regulators from around the world participated, representing institutional arrangements including formally independent regulatory institutions, ministerial regulators, and single and multi-sector regulators including those responsible for competition.

The report finds that undue pressure can be exercised at different points in the life of a regulatory agency. For example:

- 88% of the regulators who receive their budgets from the executive receive annual rather than multi-annual budget allocations, which can increase the risk of undue influence and affect their financial independence.
- Most of the regulators have their head appointed by the government's executive branch. In 15% of cases, the appointment is made by parliament. Only eight regulators use a search committee for hiring a new chair.
- Over half the regulators place no restrictions on pre- or post-employment of professional staff, opening the risk of 'revolving doors' and conflicts of interest with industry and the political cycle.
- Only a quarter of the regulators are given a government statement of expectations on their conduct. Such formal public statements can be useful to clarify roles, goals and activities in a transparent and accountable way.

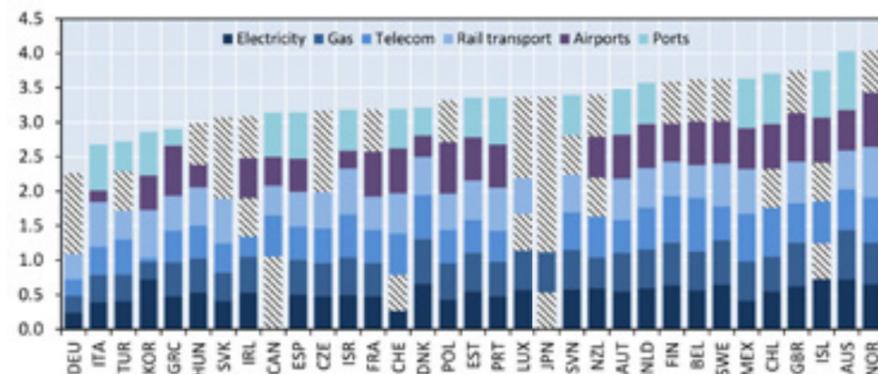


Figure 1. The governance of regulators in six network sectors: levels of independence according to the *de jure* measures in each country. Source: Koske et al., 2016.



Regulating in the dark: oversight over intelligence services

Martin Lodge considers the relationship between transparency and security

A key conclusion of this work is that regulatory independence is not an end in itself, and that it should be seen as a means of ensuring effective and efficient public service delivery by the different market players. Developing a culture of independence is just another way of nurturing better performance.

The task for government institutions and regulators is how to develop this culture of independence that delivers for users. Independence is not a static state achieved once and for all by statute. While institutional design is one part of optimizing independence, it is not sufficient. A regulator can be part of a ministry and yet be more 'independent' than a regulator in a separate body.

Building on the work conducted so far, the OECD has developed a 'pinch point analysis' methodology to highlight the critical events in the life of a regulator where undue influence and pressures can be greatest. Agency finances, staff behaviour, appointment and removal

of leadership, the way in which agency intersects with political cycles, and the interaction with the various actors in the regulatory sphere are pinch points specific to the regulator's environment. They can be amplified when two or more events occur at the same time. An example might be a political election coinciding with a rise in crude oil prices and a change in the head of the agency. It is at these critical points that action needs to be taken in order to protect regulators from undue influence.

Building on this methodology, the OECD is currently developing guiding principles for how regulatory agencies and, more generally, arm's-length bodies, can be protected from undue influence. For instance, multi-year budgets can provide predictability and shield the regulator from short term political concerns or reactions to decisions taken by the regulator. Making the nomination process more transparent can help recruit chairs and agency heads who have the neces-

sary technical skills and credibility to enhance the performance of the regulator. These institutional arrangements would not only make the agency or body more effective but also signal the willingness to protect the regulator from undue influence. This signal is the condition for nurturing a culture of independence that enables the regulator's leadership and staff to behave and act independently.

Being an independent regulator cannot mean adopting the cloak of invisibility and working behind the scenes like the Men in Black. Regulators must fully engage with all stakeholders. Maintaining independence in the midst of significant pressure from all sides requires governance structures aimed at nurturing a culture of independence.

It may not keep the galaxy safe, but it will ensure that regulatory agencies better serve the public good.

For more information see OECD (2016b, 2016c) on 'Independence of regulators and protection against undue influence' and 'Governance of Regulators' Practices'.

References

Koske, I., Faisal Naru, F., Beiter, P. and Isabelle Wanner, I. (2016) 'Regulatory management practices in OECD countries', OECD Economics Department Working Paper no. 1296, Paris: OECD Publishing. <www.keepeek.com/Digital-Asset-Management/oecd/economics/regulatory-management-practices-in-oecd-countries_5jmoqw-m7825h-en#.WAOg-DKZNIY>

OECD (2016a) *Being an Independent Regulator*. Paris: OECD Publishing.

OECD (2016b) 'Independence of regulators and protection against undue influence', <www.oecd.org/governance/regulatory-policy/independence-of-regulators.htm>

OECD (2016c) *Governance of Regulators' Practices: accountability, transparency and co-ordination*. Paris: OECD Publishing.

Filippo Cavassini, Faisal Naru and Bill Below are in the Regulatory Policy Division of the OECD.

One of the most well-known principles in the canon of Jeremy Bentham's writings on government is the general principle of transparency. All activities, according to Bentham, were to be made open so as to allow for external scrutiny. One sector, however, was exempted from this universal principle: the security or intelligence services. The reason for this exemption appears straightforward; security services, by their very nature, have to operate outside the glare of public attention in order to perform their work.

At the same time, the secrecy of operations also calls for some degree of regulation and oversight; after all, discretion can be abused – the state's covert activities to make individuals' lives transparent require disciplining constraint. The regulation of the security state is therefore a very special, and particularly tricky case for the study of the regulation of government activities. In an age where the threat of terrorism has, once again, become a feature of daily life, the regulation of intelligence services is also an area that has become increasingly important as different intelligence services have launched recruitment drives, as concerns about access to encrypted communication have escalated, and the world of digital technologies is said to fundamentally alter the nature of intelligence work, and as the context of and conditions for national and international co-operation have changed.

What then can be said about recent trends in regulation and oversight? This is arguably not a question for those fascinated by a James Bond-like glamorous lifestyle. This is more the world of political and public concern with agencies that possess extraordinary powers to interfere in private and personal

matters, that have coercive powers, and whose main objective is the minimization of threat to the state and its citizens. It is also a world in which different understandings regarding an individual's right to privacy

extremist activities such as showing a remarkable negligence in monitoring right-wing extremist sympathisers. Furthermore, the 9/11 Commission Report, and other incidents, have highlighted the difficulties of ensuring national, let alone international, information exchange. In other cases, there has been rather extensive collaboration as evidenced in the recent inquiries into the collaboration between the German BND and the US-NSA. This also links to examples of so-called intelligence failures, where information was detected, but not acted upon. Attempts in the US have remained fraught as individual agencies anxiously protect their turf vis-à-vis the Department of Homeland Security and other co-ordination initiatives. Pooling of expertise is emerging across the European Union (as part of the 'Counter Terrorism Group') after 2001, but has remained problematic given the preferences for bilateral agreements. Similar reluctance exists when it comes to national services' willingness to supply Europol with information.

Of course, problems with the (oversight of) intelligence services are far from novel – concerns with the activities of intelligence services have been a recurring feature throughout the post-1945 period, including concerns about infiltration in highest places of government (such as then West German Chancellor Willy Brandt's special advisor, Günter Guillaume), double agents (such as the infamous 'Cambridge Five') and 'cowboy' intelligence activities in diverse parts of the world (such as Jamaica and Northern Ireland). In the US, concerns about the activities of the intelligence services led to a formalization of oversight in the 1970s.

In debates over the regulation of intelligence services, one does not have to look very far to encounter the trade-off

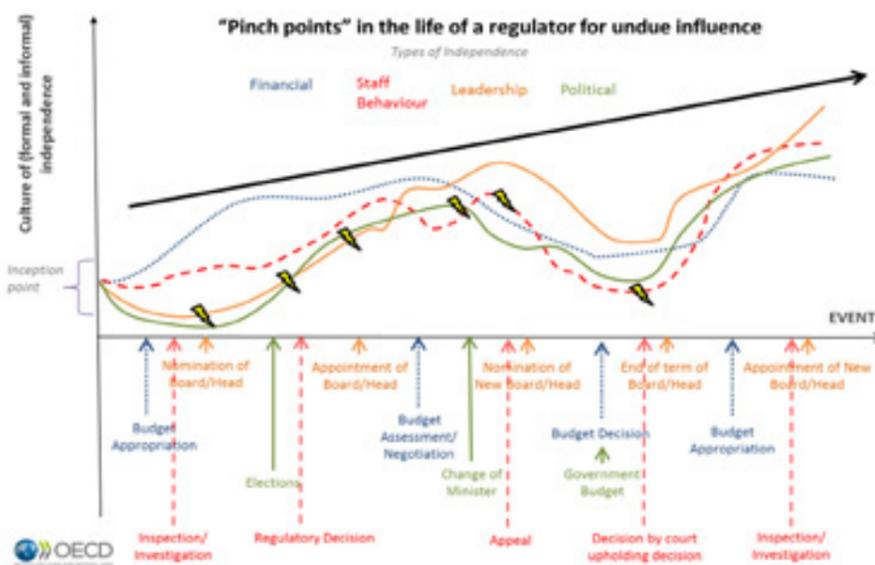
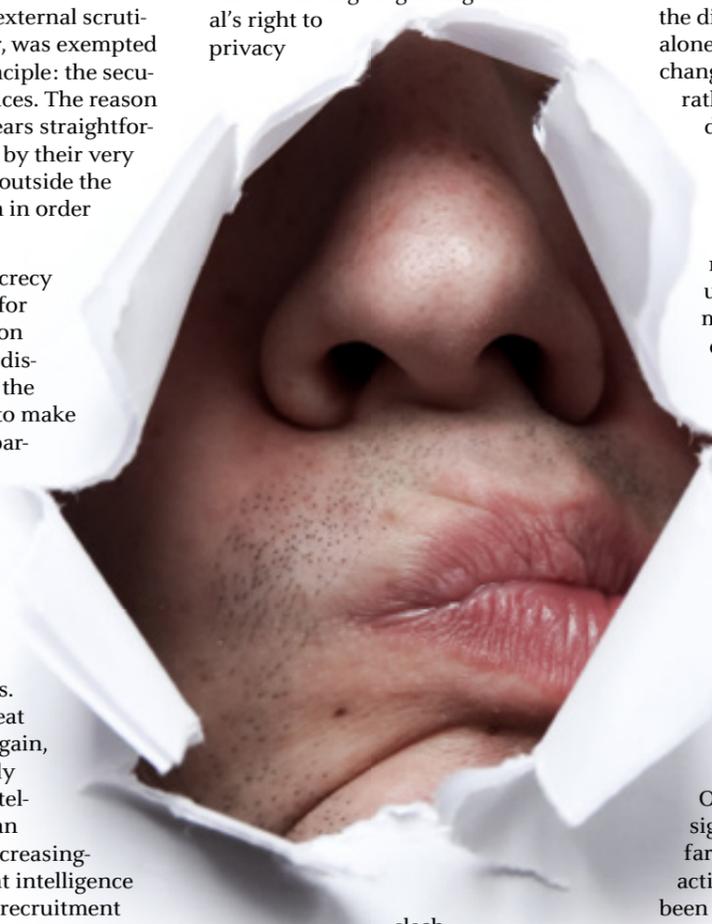


Figure 2. 'Pinch point analysis' methodology demonstrating the level of independence against events in the life of a regulatory agency or arm's-length body. The trend of independence can be positive or negative over time and where there is congruence of events there can be greater avenues for undue influence (OECD 2016a)



between the functional prerequisite to operate covertly and the 'costs' of being accountable and transparent to a sceptical political class and the wider public. Constitutional courts, such as the German federal constitutional court, have been highly critical regarding procedural protection against the abuse of discretionary powers. Courts have, therefore, become regulators in their own right.

Intelligence services are very difficult to control - neither their daily activities nor their achievements are easily observable. Only failure can be identified, and here it may have to do more with blame-avoiding behaviours of others than actual failure. There are some controls over inputs, and one may be able to assess procedural appropriateness. One traditional tool in such cases is to rely on 'professionalization'. By careful selection and training, intelligence services are supposedly committed to constitutional values. But such a strategy is somewhat problematic in an age where the priority is to massively expand and the security state relies on 'security cleared' contractors. Such bureaucratic recruitment drives are marred by severe difficulties, as noted by Rizzi and Borden in this issue.

The wider environment in which intelligence services operate has also changed. There have been traditional differences in official acknowledgement; for example, the UK intelligence services were only officially recognised in the late 1980s and early 1990s. Some intelligence services now publish their addresses, they provide some information on their websites (even pictures of their buildings), and the actual identity of their leaders is publicly known. Yet, the availability of information on budgets and staffing numbers remains less open. In contrast to the world of three or four decades ago, there has been a notable

trend towards 'voluntary accountability' to appeal to public support and legitimacy.

This emphasis on self-presentation is mirrored by extensive changes in the wider oversight ecology. There has been an increasing reliance on internal legal clearance procedures. This has, in turn, led to a considerable growth of in-house lawyers to provide advice on the legality of particular operations. Such a growth in formal legal requirements might be interpreted as a response to (the perception of) distrusting politicians and a fear of 'moral panic' about revelations regarding particular operations. To some, this juridification represents a challenge to the execution of the core functions of intelligence services.

Furthermore, there has also been a rise in external watchdogs and oversight bodies. In the US, the role of the Inspector General has changed from an earlier

age in which a position in that office was seen as a 'recovery period' from tricky intelligence operations. Instead, since 1989 when the position was placed on a statutory basis, the Inspector General has become increasingly resourceful and distant from the intelligence services.

In the UK, there has been a remarkable change in parliamentary oversight, partly in response to pressures from the European Convention of Human Rights. The first Intelligence and Security Committee (ISC) was a statutory, not a parliamentary committee; it reported to the prime minister, was hand-picked by the prime minister and operated in closed sessions, with its reports being prone to redactions. Requests for information could be refused on grounds of sensitivity. The Justice and Security Act 2013 made the ISC a committee of parliament with extended powers of oversight, and with members being appointed by Parliament (following nomination by the Prime Minister in consultation with the Leader of the Opposition).

Whatever the formal standing of legislative oversight committees, their actual role is problematic as committees are supposed to play a dual function in providing both support and oversight. A too critical oversight performance, one that is also linked to critical commentary in the media, is likely to lead to a breakdown in the relationship between the committee and the intelligence services. At the same time, too much 'cheerleading' for the intelligence services will also be seen as problematic, as is an 'ostrich' style oversight in which parliamentarians are seen to be avoiding any form of difficult confrontation - only to be the first to criticize intelligence services once issues have appeared in public).

Similarly, as noted by Amy Zegart (2011) in the case of the US, oversight is limited by a lack of interest by legislators (the oversight of intelligence services being

unlikely to be a vote-winner in constituencies) and by lack of power over budgetary appropriations. Other observers suggest that politicians might be keen to play to the gallery of public attention in times of failure and public outcry, but they will be reluctant to engage when difficult choices are presented to them. There are also questions as to how to bring together different parliamentary overseers. The latter issue has, in the German case, led to the creation of a special *Beauftragte* role in parliament, tasked with providing co-ordination between different parliamentary oversight bodies. Again, concerns have arisen as to the background of potential appointees; with 'insiders' being seen as 'too close', whereas outsiders are viewed as potentially ineffective due to lack of inside knowledge.

Regulatory overseers might not have the problem of limited political attention spans, although they face similar issues when it comes to questions of 'critical distance'. Their specific challenge therefore is to highlight to the wider public that they are engaging in active and critical oversight, without necessarily revealing the extent and the content of their interactions. How, therefore, such bodies are accountable, and how they pursue strategies of engagement with interested parties (and who is regarded as a legitimate party) remains highly controversial within and across jurisdictions.

Oversight is also problematic when it comes to international cooperation. One country's legal interpretations of international human rights conventions might differ from another country's.

Competing interpretations about human rights might be seen to stand in the way of effective cooperation. Indeed, such differences might also reflect different national traditions with regard to the role of legal advice; and such traditions will ultimately lead to further conflicts between the rival interpretations about human rights and demands for 'more cooperation'.

The powers of the intelligence state are not only relevant in view of their direct powers over individuals. Conflicts between technology companies and intelligence services have become particularly prominent in recent times over access demands to the information stored on smartphones and encrypted communication systems. Again, the issue of providing the state with a formal or even informal backdoor to technological systems is one that places competing claims about collective

security interests against each other. These conflicts link to two fundamental debates. One is the extent to which private organizations can be forced to cooperate with the security state. Such relationships require a degree of procedural formality, even if they are secretive. The other relates to the potential differences in the snooping powers of private versus public organizations. The difference in terms of the coercive powers of the state is clearly one major difference. However, this difference should not stand in the way of critical questions with regard to the use of private data and 'snooping' capacities by technology firms.

The regulation of security services in an age of international cooperation and modern communication technologies is therefore one of the most vexing problems in the regulation of contemporary executive power. The tensions identified by Bentham are impossible to design away; tensions between civil liberties and security concerns, the role of competing understandings as to what counts as evidence, how to ensure the upholding of constitutional values, and how to sustain critical, but non-adversarial oversight constitute some of the most important questions facing liberal democracy in an age where fears about security are central to the political and public agenda.

References

Zegart, A. (2011) 'The domestic politics of irrational intelligence oversight'. *Political Science Quarterly* 126(1): 125.

Martin Lodge is Director of **carr**. 'As part of the Regulation in Crisis?' seminar series, **carr** held a workshop on the regulation of homeland security, bringing together leading practitioners and academics.

The artefacts of risk management

Michael Power highlights the effortful nature of risk management practice

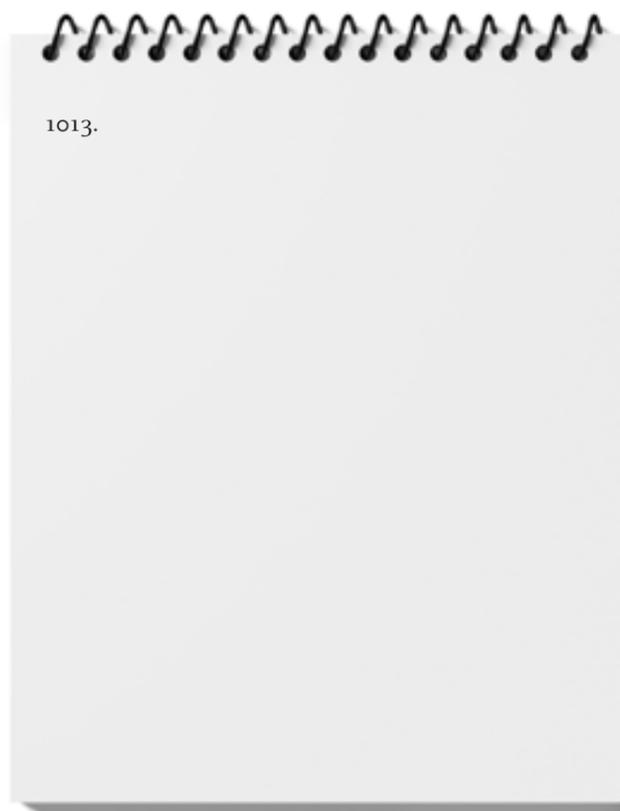
In managing risk, organizational actors are constantly engaged in the work of representing it. From a philosophical point of view, this co-mingling of risk and representation is unsurprising. Risks are contingencies or future possibilities which have not yet crystallized into events. As non-real possibilities, they literally do not exist and cannot be seen until they are represented and processed in apparatuses for their management. On this view the unreality of risk in the future can only be made real and actionable in the present by being somehow captured and represented.

So when we look closely at risk management in the field, we see that practices are littered with artefacts which contain representations of risk. Documents and records like risk maps are known to be important artefactual mechanisms through which organizational agents contribute to, visualize and sustain organizational practices over time. We also find that the work of managing risk is entangled with institutional frameworks for accountability, and we need to understand better how these frameworks emerge and shape work processes, and how organizational artefacts are arranged in infrastructures for representing and organizing this riskwork.

Routines and risk

Studies of organizational routines and of the central role played by artefacts provide the analytical and empirical

materials for how we might think about, and approach, the analysis of risk management practice. An 'arte-factual turn' in risk studies could be based on the following questions: what is the infrastructure of artefacts through which risk is routinely identified, communicated and acted upon?; how do these artefacts have agency in shaping both the risks which routinely get attention and the form of that



attention?; and how do these artefacts connect to systems of individual and organizational account giving? Put simply, these questions imply that a great deal of riskwork is done by non-human actors – the artefacts of risk management.

Take the example of the systemic risk of the financial system. While the dan-

ger existed and was conceptualized as a risk many years prior to the financial crisis, the dominant artefactual representations of that risk were in terms of the financial strength of individual banks. A huge amount of thinking was focused on the production of solvency representations and related capital issues at the level of the individual firm with the implied assumption that if the sum of financial organizations were individually sound, then the system was sound. But the interconnectivity risk associated with the wholesale inter-bank market was much less prominent and was poorly represented, leading one senior practitioner to describe the financial crisis as an 'intellectual failure'. So, following the height of the financial crisis a great deal of effort has been undertaken to correct this failure and to represent bank inter-connectedness and its associated risks, involving new kinds of models, artefacts and analyses.

Whether systemic risk is 'real' or not is a question of interest only from a certain philosophical point of view. What is of more interest is how the dan-

ger of systemic collapse has a history in which it has transitioned from one system of representation to another, with a corresponding change in the riskwork and associated systems of artefacts. We could say that the risk object (cf Hilgartner) of systemic risk always existed in some sense, but it has now been embedded in a new socio-technical network for representing and intervening

in it. As analysts, we should not rush to judge whether this is an improvement or not, although as citizens and taxpayers we rather hope so.

Artefacts and risk infrastructure

This artefactual perspective on risk management is not intended to debunk risk management practice but to understand better its processes. After all, as Atul Gawande argues in his well known celebration of the checklist as the embodiment of accumulated knowledge and expertise, real lives are saved by pilots and surgeons using well designed checklists. In these cases the artefact of the checklist is close in space and time to those making decisions about flight safety and surgical risk respectively. Following the checklist mitigates the risk of human error, imperfect memory, and unnecessary variation in the performance of a critical task and its consequences for life.

And yet, even in this worthy example, a checklist is a more complex artefact than it first appears. Firstly, the form of the checklist often has a distinct history, usually emerging from post-accident investigations and analyses. Secondly, the checklist as an artefact may not have an organizational life solely for the benefit of in situ pilots and surgeons. It may persist as an organization record allowing others to judge compliance or to conduct an investigation. In short, the checklist may exist in a system of linked artefacts which make the actions of the pilot and surgeon visible and accountable to others – hospital and airport managers, investigators, regulators, and so on.

So, on the one hand, there seem to be artefacts like Gawande's checklists which embody a clear purpose and which are co-extensive with managing risk. On the other hand, there seems to be a class of artefacts which are systematically organized to build up accounts of performance or to permit forensic ex post investigation of performance. These artefacts have a different

organizational trajectory from the first kind; they can move very far from the routines with which they are associated and become aggregated as performance representations which are stored and subject to further analysis.

The empirically interesting artefacts, such as risk registers, sit at the boundary between the first order management of risk and these wider systems for performance accountability. They generate critical questions such as: under what conditions do organizational actors become distracted by this forensic role of risk management artefacts?; what might be the consequences of such a shift in their attention?; could these consequences, understood broadly as the risk of accountability 'crowding out' performance, themselves be represented within the risk management system?

In general, the system of artefacts approach being proposed recognizes that organizational actors who engage in the routine management of risks are also producing artefacts whose trajectory constitutes the 'regulated life' of an organization and in which traces of their work are inscribed. In turn, such traces make the work of risk management auditable by others; riskwork at the granular level may therefore often implicate auditwork.

Riskwork and auditwork

The strength and effects of a so-called 'logic of auditability' in risk management, and its embeddedness in a connected system of artefacts, are matters for empirical enquiry. For many years, risk management scholars have been concerned about whether the tail of audit and accountability, and possible blame, wag the dog of risk management. Many studies suggest that organizational agents focus as much on managing the risks to themselves and their reputations by constructing defensible audit trails which may actually increase overall risk.

Yet, while there is a general awareness of this issue both by scholars and also

by those who work in regulation and risk management, borrowing the 'arte-factual turn' from routines theory encourages analysis to move beyond general assertions about 'blame avoidance', 'reputation management', or 'legitimation' strategies in characterizing the side effects of accountability for risk management. The system of artefacts perspective strengthens the analytical and empirical focus on how specific artefacts shape both attention and action in the risk management field. In short, I propose that an artefactual turn within risk studies supports a possible empirical programme focused on the dynamic relation between what I call 'auditwork' and 'riskwork'.

Finally, an essential tension between action and representation exists at the heart of all organizational routines. It gives them their dynamic properties and this is especially true for the routines that constitute risk management practices. Situated human actors navigate the so-called 'risks of risk management' posed by a world of artefacts and as analysts we have an opportunity to observe their skill and effort, sometimes resisting and sometimes succumbing to a logic of auditability which can be pervasive and powerful. The different contributions to *Riskwork: essays on the organizational life of risk management* (Oxford University Press, 2016) provide a body of evidence about the effortful nature of risk management practice in many different settings. Routines theory provides the conceptual apparatus and empirical sensibilities to take this agenda further.

This is an abbreviated version of the essay 'Postscript – on riskwork and auditwork' in Michael Power (ed.), *Riskwork: essays on the organizational life of risk management*, Oxford: Oxford University Press, 2016.

Michael Power FBA is Professor of Accounting at the London School of Economics and Political Science and a former Director of **carr**.

carr news

We welcome two new research officers to **carr**. **Alex Griffiths** joins us from King's College London as research officer on the QUAD project. He has also worked at the Care Quality Commission. **Jeremy Brice** joins us from Newcastle University. We say farewell to **Kavita Patel**, TransCrisis project manager, who is leaving us to pursue a career in scriptwriting for television.

Congratulations to **Mike Power** who has been elected as Fellow of the British Academy. He is the first accounting academic to receive this prestigious fellowship. He was also awarded an honorary doctorate at the University of Turku.

carr has received funding under the UK Prosperity Fund for a study on the regulation of logistics infrastructures in Brazil. Partners in the project are IPEA and RAND Europe.

carr publications

Competition and regulation in electricity markets

Edited by Sebastian Eyre (with Michael G. Pollitt), Cheltenham: Edward Elgar

Measurement instruments and policies in Africa

Lydie Cabane (with Josiane Tantchou), *Revue d'anthropologie des connaissances* 10 (2)

Mesurer et standardiser : les technologies politiques du gouvernement de l'Afrique

Lydie Cabane (with Josiane Tantchou), *Revue d'anthropologie des connaissances* 10 (2)

Quantifying, economising, and marketing: democratising the social sphere?

Liisa Kurunmäki, Andrea Mennicken and Peter Miller, *Sociologie du travail*, doi: 10.1016/j.soctra.2016.09.018

Reputation and accountability relationships: managing accountability expectations through reputation

Martin Lodge (with Madalina Busuioc), *Public Administration Review*, doi: 10.1111/puar.12612.

Riskwork: essays on the organizational life of risk management

Edited by Michael Power, Oxford: Oxford University Press

The rationality paradox of nudge: rational tools of government in a world of bounded rationality

Martin Lodge (with Kai Wegrich), *Law & Policy* 38 (3): 250–67

What is regulation? An interdisciplinary concept analysis

Martin Lodge (with Christel Koop), *Regulation & Governance*, doi: 10.1111/rego.12094.

carr discussion papers

Regulation scholarship in crisis?

Edward Balleisen, Caelesta Braun, Cary Coglianese, Diogo Coutinho, Flavia Donadelli, Hanan Haber and Eva Heims, Christel Koop and Scott James, David Levi-Faur, Kenneth Abbott and Denis Snidal, Martin Lodge, John McEldowney, Fabiana Di Porto, Henry Rothstein, Colin Scott, Lindsay Stirton, Slobodan Tomic, Andy Whitford and Gary Miller, Karen Yeung.

Innovation through customer engagement and negotiation settlements in water regulation: towards a transformed regulatory state?

Eva Heims and Martin Lodge

carr seminars

Better regulation: the Business Impact Target and the way forward

Jointly held with the National Audit Office

Anne-Marie O'Riordan and Richard Davis (National Audit Office), Steve Darling (Department for Environment, Food and Rural Affairs), Henry Demaria (Department for Communities and Local Government), Claudio Radaelli (Exeter), Graham Turnock (Better Regulation Executive)

October 2016

Independent regulators

Faisal Naru and Filippo Cavasini (OECD)

October 2016

carr events

As part of the ESRC-funded 'Regulation in Crisis?' seminar series, **carr** organised two major international workshops. One workshop focused on the 'Regulation of Homeland Security' and brought together leading international practitioners and academics to discuss the changing nature of oversight over intelligence services.

A second event focused on the issue of 'Scholarship on Regulation In Crisis?'. This workshop discussed how scholarship on regulation had been shaped by the financial crisis, how theories of regulation required reconsideration, and how new fields of regulation were posing challenges for existing theories. Participants in this workshop included Edward Balleisen (Duke), Caelesta Braun (Leiden), Madalina Busuioc (Exeter), Cary Coglianese (Pennsylvania), Diogo Coutinho (São Paulo), Flavia Donadelli (LSE), Hanan Haber (LSE), Eva Heims (LSE), Will Jennings (Southampton), Christel Koop (KCL), David Levi-Faur (Jerusalem), John McEldowney (Warwick), Fabiana Di Porto (Salento), Henry Rothstein (KCL), Colin Scott (UCD), Lindsay Stirton (Sussex), Andy Whitford (Georgia) and Karen Yeung (KCL)

The QUAD consortium had its second meeting in Paris in September.

The TransCrisis consortium met in Stockholm in September to discuss progress across the different research activities. In particular, it focused on work on two work packages; research on the institutional capacities of the European Commission in terms of crisis management, and work on 'backsliding' in EU norms and provisions across member states. The meeting also included a contribution by Claus Sørensen, former director-general of Humanitarian Aid and Civil Protection, and Communication in the European Commission.

carr talks

Lydie Cabane was a discussant at the seminar 'Shaping Crisis, Devices, Technologies and Organizations', IFRIS in Paris in October.

Bridget Hutter has been appointed to the Environment Agency's Long-Term Investment Scenarios Development Group. She has also been appointed as chair of the Scientific Advisory Board of the Nordic Societal Security research programme and in June attended a meeting of the Scientific Advisory Board and Annual Conference of the Nordic Societal Security research programme, Reykjavik. In September, she participated in an early career workshop on 'The Opportunities Practicalities and Constraints of Socio-Legal Scholarship' at the European University Institute (EUI).

Martin Lodge presented papers at the ECPR European Union conference in Trento on 'salience and transboundary crisis management regimes' (with Lydie Cabane), at the ECPR Regulation & Governance conference in Tilburg on 'transparency and transnational regulation' (with Christel Koop), at the PMRC conference in Aarhus on 'reputation and transparency' (with Madalina Busuioc), at the IPSA conference in Posnan on 'customer engagement and the regulatory state' (with Eva Heims) and at the APSA conference in Philadelphia on 'exit or loyalty: dynamics in local authority inspections' (with Chris van Stolk). In September, he was also keynote speaker at the 'Governance, Innovation and Development' conference organized by the Brazilian civil service school ENAP and the Brazilian Ministry of Planning.

Andrea Mennicken organized, with Mike Power, a workshop on 'Accounting, Fact, Value' at the LSE in May. She presented papers at the EGOS conference in Naples on 'dynamics and limits of regulatory privatization: audit quality control in Russia, 1985–2015'

(with Anna Alon and Anna Samsonova-Taddei), at the SASE conference in Berkeley on 'the quantification of decency' and 'quantifying, economizing, and marketizing' (with Liisa Kurunmäki and Peter Miller) and at the 4S/EASST conference in Barcelona on 'financialization, organization and the emergence of asset impairment rules' (with Yuval Millo). In October, she was an invited speaker at the conference 'Collecting, Sorting, Ordering: Practices of Listing in Popular Culture' at the University of Siegen.

Peter Miller gave an invited plenary address to the World Congress of Accounting Historians in Pescara, Italy, in June on the theme of 'Towards a genealogy of failure'. He presented a paper on 'Quantifying and valuing life at the margins: healthcare and correctional services' (with Liisa Kurunmäki and Andrea Mennicken) at the 4S/EASST conference in Barcelona.

Mike Power presented together with Andrea Mennicken a paper on 'Valuation wars: competition and conflict between IASB and IVSC' at the Competitions workshop, Copenhagen Business School, in June. He gave the keynote addresses at the Risk Summit at Cambridge University in June on the theme of 'Risk culture and information culture' and at the Culture Summit at Holyrood (Edinburgh) in August on 'Culture on the edge'. He also contributed to a conference on university governance in Hannover on 'The impact agenda in research governance'.

carr directorate

Martin Lodge
Director of carr; Professor of Political Science and Public Policy, Department of Government

Andrea Mennicken
Deputy Director of carr, Associate Professor of Accounting, Department of Accounting

carr research staff

Jeremy Brice
carr/FSA Research Officer

Lydie Cabane
TransCrisis Research Officer

Alex Griffiths
QUAD Research Officer

carr senior research associates

Bridget Hutter
Professor of Risk Regulation, Department of Sociology

Peter Miller
Professor of Management Accounting, Department of Accounting

Michael Power
Professor of Accounting, Department of Accounting

carr research associates

Michael Barzelay
Professor of Public Management, Department of Management, LSE

Elena Beccalli
Professor of Banking, Faculty of Banking, Finance and Insurance, Università Cattolica del Sacro Cuore, Milan

Matthias Benzer
Lecturer in Sociology, Department of Sociological Studies, University of Sheffield

Daniel Beunza
Assistant Professor of Management, Department of Management, LSE

Gwyn Bevan
Professor of Policy Analysis, Department of Management, LSE

Julia Black
Interim LSE Director, Professor of Law, Department of Law, LSE

Adam Burgess
Professor of Risk Research, School of Social Policy, Sociology and Social Research, University of Kent

Madalina Busuioc
Senior Lecturer in Politics, Department of Politics, University of Exeter

Yasmine Chahed
Lecturer in Accounting, Department of Accounting, LSE

Damian Chalmers
Professor of European Union Law, Department of Law, LSE

David Demortain
Research Fellow, IFRIS, University of Paris-Est

Flavia Donadelli
LSE Fellow, Department of Government, LSE

John Downer
Lecturer in Risk and Resilience, School of Sociology, Politics and International Studies, University of Bristol

Hanan Haber
LSE Fellow, Department of Government, LSE

Matthew Hall
Professor of Accounting, Department of Accounting, Monash Business School, Monash University

Eva Heims
Lecturer in Public Policy, Department of Politics, University of York

Michael Huber
Professor of Sociology, Faculty of Sociology, Bielefeld University

Will Jennings
Professor of Political Science and Public Policy, University of Southampton

Silvia Jordan
Associate Professor of Accounting, Department of Accounting, Auditing and Taxation, Innsbruck University

Roger King
Visiting Professor at the School of Management, University of Bath

Mathias Koenig-Archibugi
Associate Professor of Global Politics, Department of Government, LSE

Christel Koop
Lecturer in Political Economy, Department of Political Economy, King's College London

Liisa Kurunmäki
Associate Professor of Accounting, Department of Accounting, LSE

Javier Lezaun
James Martin Lecturer in Science and Technology Governance, and Deputy Director of the Institute for Science, Innovation and Society, University of Oxford

Sally Lloyd-Bostock
Visiting Professor, Department of Sociology, LSE

Donald MacKenzie
Professor of Sociology, School of Social and Political Science, University of Edinburgh

Carl Macrae
Senior Research Fellow, Department of Experimental Psychology, Medical Sciences Division, University of Oxford

Kira Matus
Senior Lecturer, Department of Science, Technology, Engineering, and Public Policy, University College London

Linsey McGoey
Senior Lecturer in Sociology, Department of Sociology, University of Essex

Anette Mikes
Professor, Department of Accounting and Control, HEC Lausanne

Yuval Millo
Professor, Accounting Group, Warwick Business School, University of Warwick

Juan Pablo Pardo-Guerra
Assistant Professor of Sociology, Department of Sociology, University of California San Diego

Edward C. Page
Sidney and Beatrice Webb Professor of Public Policy, Department of Government, LSE

Tommaso Palermo
Lecturer in Accounting, Department of Accounting, LSE

Bartholomew Paudyn
Fellow, Department of International Relations, LSE

Nick Pidgeon
Professor of Environmental Psychology, School of Psychology, Cardiff University

Tony Prosser
Professor of Public Law, University of Bristol Law School, University of Bristol

Henry Rothstein
Senior Lecturer in Risk Management, Department of Geography and Deputy Director of King's Centre for Risk Management, King's College London

Rita Samiolo
Assistant Professor of Accounting, School of Management, Innsbruck University

Susan Scott
Associate Professor of Information Systems, Department of Management, LSE

Nick Sitter
Professor of Public Policy, Department of Public Policy, Central European University

Kim Soin
Associate Professor of Accounting and Management, University of Exeter Business School, University of Exeter

Lindsay Stirton
Professor of Public Law, Sussex Law School, University of Sussex

Brendon Swedlow
Associate Professor of Political Science, Department of Political Science, Northern Illinois University

Peter Taylor-Gooby
Professor of Social Policy, School of Social Policy, Sociology and Social Research, University of Kent

Mark Thatcher
Professor of Comparative and International Politics, Department of Government, LSE

Zsuzsanna Vargha
Lecturer in Accounting and Organization, School of Management, University of Leicester

Frank Vibert
Senior Visiting Fellow, Department of Government, LSE

Leon Wansleben
Assistant Professor of Sociology, Department of Sociology, LSE

Kai Wegrich
Professor of Public Administration and Public Policy, Hertie School of Governance, Berlin

carr visiting fellows

Elena Bechberger
Senior Policy Advisor, NHS Improvement

Charles Borden
Partner, Allen & Overy, Washington DC

Anneliese Dodds
MEP for South East England

Julien Etienne
ICF International

Sebastian Eyre
Head of Energy Regulation, EDF Energy

Ed Humpherson
Head of Assessment, UK Statistics Authority

Jeremy Lonsdale
Director, National Audit Office

carr administration

Yvonne Guthrie
Centre Manager

Justin Adams
Seminars

Muhammed Iqbal
Web, Publications and Discussion Papers

Sala Ud-Din
Reception

carrseat production

James Robins

carr researchers

Julia Batistella-Machado
Research Assistant, Regulation of Logistics Infrastructures in Brazil

carr interns

Martina Bedatsova
Michael Czarnota
Irene Ferrandiz-Merino
Joel Pearce

