WHAT'S IN A MODEL?
COMPUTER SIMULATIONS AND THE MANAGEMENT OF IGNORANCE

EUGENIA CACCIATORI
Cass Business School, City, University of London
eugenia.cacciatori@city.ac.uk

PAULA JARZABKOWSKI
Cass Business School, City, University of London
Paula.Jarzabkowski@city.ac.uk

REBECCA BEDNAREK
Victoria University of Wellington
rebecca.bednarek@vuw.ac.nz

KONSTANTINOS CHALKIAS
Birkbeck, University of London
k.chalkias@bbk.ac.uk

INTRODUCTION

There is growing interest in how material objects mediate organizational activities (Carlile, Nicolini, Langley, & Tsoukas, 2013; Leonardi, Nardi, & Kallinikos, 2012). Much of this interest centers on how artifacts represent knowledge and the effects of this representation on the creation, sharing, and use of knowledge as well as the coordination of action (e.g. D'Adderio, 2001; Carlile, 2002; Bechky, 2003; Cacciatori, 2012; Jarzabkowski, Bednarek and Spee, 2015). In this paper, we suggest that this focus on knowledge can be usefully complemented by a focus on ignorance, namely how artifacts mediate organizing in the face of what is not known, or of knowledge that cannot be shared. We pursue this line of enquiry by looking at the development and use of a specific type of artifact, computer simulations, in the context of terrorism insurance. Simulations are mathematical models embedded in computer programmes that calculate numerical solutions under a wide range of conditions (e.g. Sundberg, 2009; Winsberg, 2003), providing summaries of these results in various ways (e.g., charts, graphs, tables, pictures and animations). They extend the reach of traditional models to cases in which analytical solutions cannot be easily calculated or interpreted; act partly as substitute of physical experiments (Morrison, 2009; Bailey, Leonardi, & Chong, 2010; Becker, Salvatore & Zirpoli, 2005); and also mediate stakeholder interactions (e.g., Galison, 1996; Dodgson, Gann & Salter, 2007). This focus on ignorance provides a new insight into how artifacts, and in particular simulations, can aid decision making both within (e.g., Bailey et al., 2012) and between (e.g., Dodgson et al., 2007) organizations, and ultimately how they affect the wider organizational processes within which they are used (Bailey et. al., 2010).

BEYOND IGNORANCE AS NON-KNOWLEDGE

Ignorance in organizing has been treated primarily as 'non-knowledge', in the form of either absence or incompleteness of knowledge, or 'distorted knowledge' such as for instance erroneous knowledge or biases. Consequently, organizational research has primarily seen ignorance as a dysfunctional aberration (Davies & McGoey, 2012; Schaefer, 2018) that needs to be reduced, corrected or kept at bay (Proctor, 2008; Smithson, 1989). Recently, a growing body of research on ignorance in the social sciences (Gross & McGoey, 2015; Proctor & Schiebinger, 2008; Smithson, 1989) and organizational studies more specifically (Bakken & Wiik, 2018; see also Davies & McGoey, 2012; Roberts, 2013; Schaefer, 2018) has advanced understanding by moving beyond Western culture's traditional disregard for the complexities of ignorance (Proctor, 2008; Smithson, 1989).

This has produced several classifications of ignorance that offer useful ways to approach its study. Proctor (2008), for example, identifies three major types of ignorance. First, as discussed above, ignorance can be seen as non-knowledge, specifically as a 'native state' or 'not-yet-knowing' (Tuana, 2004). Ignorance in this sense is a powerful motivation for the pursuit of knowledge – and indeed the science system is kept alive by a constantly renewing pool of ignorance, in which each discovery generates new questions (Merton, 1987). Second, ignorance can be seen as a 'lost realm' that derives from selective choices about what to study and what not to study. In this sense, ignorance is a 'declaration of irrelevance' (Smithson, 1989). Ignorance appears to be here a by-product of knowledge and its pursuit. Third, ignorance is an active construct, in many cases as 'strategic ploy', as, for example in the case of trade secrets, or the selective withholding of information for security reasons (e.g. Kutsch & Hall, 2010; Rappert and Balmer, 2015). Within this category, there is also ignorance that is enforced for moral reasons, such as privacy, and taboos as a form of 'socially enforced ignorance' (Smithson, 1989).

Recent reviews (Proctor, 2008; Smithson, 2008) consequently conclude that ignorance is not simply 'a void' beyond the limits of current knowledge that waits to be filled, but "is a pervasive and fundamental influence in human cognition, emotion, action, social relations and culture" that sustains social life from polite conversation to peer review in science (Smithson, 2008: 209). Yet, there have been few studies that link ignorance to 'concrete examples' (Gross, 2007). There has consequently been a corresponding call for studies of ignorance as a topic of interest in organization studies (Bakken & Wiik, 2018). In this paper, we therefore investigate the role of artifacts not as mediators of knowledge creation and exchange as in the previous literature, but as mediators in the organizational processes through which ignorance is managed.

SETTINGS AND METHODS

We address the role of artifacts in the management of ignorance via a study of terrorism risk simulation models in the context of delivering terrorism insurance products. The business of insurance is viable in the grey zone between perfect knowledge of who and when will be subjected to a loss and complete ignorance. While statistics is crucial in managing ignorance in this gray area, the practice of underwriting is guided by a variety of other mechanisms, so that "scientific data on risk are variously absent, inadequate, controversial, contradictory, and ignored" (Ericson & Doyle, 2004a, p.137-8). This fact and the extensive use of modelling techniques to assess risk make insurance an excellent setting for our investigation.

Given the globally interconnected nature of both terrorism and terrorism insurance, during 2016-2018 we conducted 106 interviews with insurers, reinsurers, brokers, modelers, governments, intergovernmental organizations, and private-public partnerships across several countries. We interviewed those most involved in developing and using terrorism models and collected numerous documentary data including reports, internal documents, and various media articles. We returned the field in 2018 (and ongoing in 2019) to conduct some additional interviews and targeted observations of terrorism modelling and underwriting.

Our analysis moved from broad sensitizing categories or indexing, to more fine grained thematic analysis (Gioia, Corley, & Hamilton, 2013), to a more interpretive theorization of that analysis (Wolcott, 1990). First, we uploaded the data in NVivo11 and coded around two broad themes: (1) the flawed nature of terrorism models; (2) use of terrorism models. These themes, which sometimes seemed counterintuitive, emerged from the data. We therefore turned to the literature, to better inform ourselves on why people might use models, even where they acknowledged their flawed nature. This initial analysis became the basis for all our following layers of analysis, which are more emergent in nature (such as compartmentalization) and reflect the themes raised by interviewees – such as the issues surrounding the strategic use of ignorance.

FINDINGS

Industry players generally have little faith in the knowledge embedded in terrorism simulation models (hereafter 'terrorism models'): "*I mean have you come across a good terror model? Who has one? ModellingCompany1 don't have one. … We don't have one, ModellingCompany2 don't have one. Do BrokerCompany1? I don't know. They just don't exist.*" (Interview). At the root of this negative attitude towards terrorism models is the need to deal with terrorist's 'adversarial human agency'. Unlike natural catastrophes, terrorism is characterized by human agency that aims at defeating defences and at causing as much damage as possible. This makes addressing adversarial agency a key issue in modelling,

while at the same time bringing terrorism modelling out of the domain of natural sciences, into areas where interviewees feel ignorance is fundamentally untamable. As one participant explained to us: *"I can say that as to the modelling there were huge differences between how you modelled the more scientific perils such as earthquake and flood with terrorism. We were always the ones that no one understood and no one really kind of trusted, because they said: How can you model human behavior."* (Interview)

As discussed above, insurance tames ignorance processing it as risk, in the form of a set of possible events (or 'states of the world') with an associated set of losses ('severity'), and probabilities of occurrence. These form the basis of actuarial modelling, including models based on simulations such as the one discussed here. However, because the trigger of terrorism is human agency, and not the 'natural' world, many interviewees perceived the estimation of probability to be outside of the realm of 'science': *"I think people have a view of probabilities - but they're not rooted in science."* (Interview). Despite the existence of some sophisticated models that take into account expert opinion as well as other publicly available information such as the number of plans foiled by security, probabilities are given very little credence: *"You know, the commercial models, ModellingCompany1 thinks that they have a probability, I mean it's laughable..."* (Interview).

Another critical area of ignorance, which some thought was the fundamental one, relates to what constitutes a credible terrorism threat given the current security environment and the international situation. *"The expertise that's very difficult is what's the latest terror threat ... The commercial models, I love it because ModellingCompany1 sits there and they go well, you know, ... we put a ten ton bomb on top of [one of the signature skyscrapers]. Well how ... realistic is that? ... Because getting ten tons of ammonia nitrate or TNT, how probable is that in this security world: none at all."* (Interview)

The difficulty in estimating possible states of the world is linked to a final source of ignorance that is distinctive of the terrorism peril: secrecy. Information related to what governments believe are credible terrorism threats and the defences against them cannot be easily made public, as terrorist would adapt and attempt to defeat them. As one participant described: *"What you really need is the government to say right, well we think these are the credible threats and this is what we're planning against. But ... you don't necessarily as a government want to reveal what you think it is that you know about the enemy. So it is genuinely difficult for government to share that information."* (Interview)

Despite these misgivings, there is extensive modelling activity in the industry. The major modelling companies all offer a terrorism model, and several players in the industry have developed their own. This suggests that, despite their shortcomings, models still play a role in helping to manage the terrorism peril from an insurance perspective. We show below that part of this usefulness derives from the way models make the management of ignorance possible.

Using models to manage ignorance: Compartmentalization and workarounds

One implication of the ignorance described above is that the estimates provided by the models show a lot of discrepancy and variation, in turn requiring a lot of organizational interpretation to use models as basis for action. *"Modelling is not a universal one size fits all, you know ... a lot of it is based on how an individual company perceives the risk and the tolerances they set for the risk and how they decide to model that risk."* (Interview)

One key way in which organizations work through ignorance to develop these interpretations is through what we have labelled compartmentalization. Participants generally noted that terrorism models are poor tools for (absolute) pricing, as this requires estimation of probabilities for the properties of individual clients. However, terrorism models have other

uses. For instance, to calculate how much capital they need to hold in reserve, insurance companies need to calculate their exposure in the form of a maximum aggregate loss across their portfolio. While still limited, terrorism models were considered good enough to estimate exposure: *"So now the problem with terror is that so far models are not really reliable, because when there is a human implication, well you don't know. ... what we monitor very precisely is our maximum exposure."* (Interview). This enabled industry participants to avoid the issue of probabilities *"We do a whole heap of scenarios but we've never put a probability on any of those because, well we just don't know"* (Interview). In this sense, modelling appears to be a key tool to compartmentalise ignorance. The use of models allowed actors to move from a situation in which terrorism is 'uninsurable' because of the untamable nature of ignorance around adversarial human agency, to partitioning that ignorance into different components that can be dealt with differently.

In addition, when it came to modelling for pricing purposes, some participants were less concerned with the absolute level of pricing than with its relative level – they were concerned with ensuring that 'high risk' clients payed more than low risk clients, in a proportionate way. *"Yes, you can't price it from an absolute perspective ... but you can do it from a comparative basis and say the risk in [postcodeA] is worth X in comparison to what it's worth in [postcodeB].... But that's what we have to do, we have to make sure that if we're charging somebody at a certain price in a certain place, then that's based on some underwriting logic and it's also fair in comparison to what everybody else ... is paying."* (Interview)

These uses of models show that the compartmentalization of ignorance afforded by terrorism models enables actors to pursue the selective coupling of modelling to specific uses through strategies of accepting or ignoring ignorance. Users of models are able to accept the untamable nature of ignorance about probabilities by uncoupling the use of models from the activities that are most sensitive to probabilities; absolute pricing. Ignorance about the possible states of the world was, by contrast, ignored, with models used to calculate exposure in worst case scenarios, which might include very unlikely forms of attack. Having an estimate of exposure, in turn, made it possible to calculate a price. So, while the use of the model is formally uncoupled from pricing, it still ends up facilitating the calculation of prices in a roundabout way through the coupling with the calculation of exposure. This compartmentalization enable actors to tackle areas of untamable ignorance in an indirect way using these models.

Using models to uncover ignorance and manage ignorance strategically

Models also enable the strategic maintenance of ignorance by acting as filters that aggregate information in a way that makes it less sensitive from an anti-terrorism perspective. Different strategies can be seen at work in different places. For example, one interviewee told us: *"So there are some quite tricky issues [for the government to share information with the organization], and so one way of getting round it could be for government to just hint and let [the organization] crack on ... and make its own deductions and do a whole load of modelling, it then shares it with government, government will then not be drawn on whether they think that's right or wrong, but will then sort of give a sort of nod and go yes, well we think that's in the right direction."* (Interview). In this case, ignorance is maintained by supporting modelers to produce a picture whilst not discussing the specifics of threats. In another case, a more structural solution was achieved in which the modelling organization was a sub-department of the government that had security clearance and held a database of potential targets, considered to be security sensitive information, in a secure area. They would run their model and then share the results with other stakeholders, but the modelling

organization would not allow stakeholders to access the data: "*So I give them modelled outputs. So they don't run the model. The model resides here in our secret area... We only pass them modelled outputs.*" (Interview)

Inter-organizational discussion about modelling is also a means of uncovering ignorance, in the sense of helping certain stakeholders identify areas of ignorance of which they were previously unaware. For example, engaging government in discussion (as shown above) gives governments a chance to become aware of what they do not know. As one of our interviewees explained "*There is nowhere in government where they are looking at these terrorist events in terms of economic loss. ...So [this organization] then have to model the type of likely and perhaps less likely scenario, so they can then turn round to government and say fine ... but understand what that means. Because currently, you know, we would be able to cover these events but then there are all those events that would remain outside and you would then have to come in and pick up the bill.* (Interview)

In summary, models provide a structured way to engage the government and industry in conversation. Such conversations enable the strategic preservation of ignorance, even as it allows industry to gain some validation of their modelling assumptions from government. Once the modelling is done, these interactions then allowed industry to reflect back to government a particular 'modelled' way of thinking about terrorism. These iterative conversations over modelling enable the uncovering of ignorance in ways that reinforce both parties interest in using models, despite their flaws as rational tools (Jarzabkowski & Kaplan, 2015), as one means of responding to terrorism risk.

DISCUSSION AND CONCLUSIONS

The idea for this paper started from a puzzle we encountered in the field: almost nobody trusted terrorism models, yet most actors were engaged in either building or using them. These findings seemed at odd with much of the organizational literature on artifacts as part of expert practices, which focuses on how artifacts mediate the dynamics of knowledge (e.g. Bailey et al., 2012; Dodgson et al., 2007; Jarzabkowski et al., 2015).

There are many possible explanations for the development and use of terrorism models even when there is little trust in the knowledge embedded in them. Scholars have long noticed that organizations request and produce vastly more information than they actually use and have associated this to a Western culture and structural features that privilege projections of rationality (Cabantous & Gond, 2011; Jarzabkowski & Kaplan, 2015; Langley, 1989; Feldman & March, 1981). From this perspective, we may understand modelling in our context, despite its flaws, as a reliance on the 'technologies of rationality' (Jarzabkowski & Kaplan, 2015; March, 2006) through which managers seek to counteract their ignorance. In particular, modelling provides reassurance to stakeholders that they can 'know' their risk, in the absence of other ways to validate their knowledgeability in relation to that risk; the process of decision making via modelling is used as a proxy for knowledge (Cabantous & Gond, 2011; Cabantous, Gond, & Johnson-Cramer, 2010; March, 2006). Similarly, work in the social studies of finance suggests that the accuracy or veracity of models might count for little when they are effective as coordination and communication devices that allow a market to function (MacKenzie & Spears, 2014; Millo & MacKenzie, 2009). We saw elements of this in our setting, in that potentially important areas of ignorance in the models, such as what is a credible threat, were collectively ignored in the interest of making the market work. Indeed, the way that models perpetuate ignorance by focusing development upon those areas of ignorance that are accepted, over those that are ignored, points to the performativity of modelling on actors' decision making (Cabantous & Gond, 2011), which even inaccurate models may be used to drive the development of a market (MacKenzie, 2008). While these

explanations have merit in our context, our findings highlight that what models allow actors to do in relation to what is not known (ignorance), and the way that interacts with what is known or becomes knowable through the model, plays an important role in their usefulness. The development and use of simulations models does not simply contribute to the banishing of ignorance by generating and spreading more knowledge, but also contribute to the maintenance of areas of ignorance for strategic reasons, as well as facilitating the development of knowledge in certain areas while contributing to the persistence of ignorance in others. We propose that models generate this dynamic interplay between knowledge and ignorance, which in turn supports their role as artifacts enabling action in areas of extreme uncertainty.

ACKNOWLEDGEMENTS

REFERENCES AVAILABLE FROM THE AUTHORS