Geoforum 64 (2015) 130–137

Contents lists available at ScienceDirect

Geoforum

journal homepage: www.elsevier.com/locate/geoforum

Data, interface, security: Assembling technologies that govern the future

Nathaniel O'Grady

University of Southampton, University Road, SO17 1BJ, United Kingdom

ARTICLE INFO

Article history:
Received 15 December 2014
Received in revised form 9 March 2015
Accepted 18 June 2015
Available online 24 June 2015

Keywords:
Interface
Risk
Emergency governance
Data
Fire and Rescue Service
Security

ABSTRACT

Over the last decade, fire governance practices in the British Fire and Rescue Service (FRS) have undergone fundamental transformation. Rather than just being responded to as and when they occur, the FRS have adopted a range of anticipatory governing strategies to govern fires in anticipation of their occurence. This turn towards anticipatory governance has been facilitated in no small part by the digital infrastructure now embedded in the FRS. Composed of data, hardware, software, fibre-optic cables along with human analysts and organisational processes, this infrastructure operates to make risk projections on fire which shape and condition strategic decision making. This paper explores the operation of this digital infrastructure through the notion of interface. Drawing on empirical material relating to processes of data sourcing and risk calculation, interfaces account for the sites, moments and experiences in which human and non-human agents relate to one another in making fire risk projections. Showing relations to exist spatially, temporally and sensually, I argue that interfaces are crucial to the operation of an anticipatory security apparatus which relies on digital devices.

1. Introduction

Recent years have witnessed dramatic transformations in emergency response across Britain. As literature which explores emergency response claims (Adey and Anderson, 2011, 2012; Anderson, 2010), these transformations fundamentally revolve around the way in which emergency response authorities both think of, and attend to, emergencies. Events such as fires, health emergencies and crime are now articulated as risks of the future. Known through risk, authorities have developed forms of action such as prevention, protection and preparedness which work to secure emergencies before they occur (Amoore, 2014; Collier, 2008, de Goede, 2013). This turn towards the anticipatory governance of emergencies, in which emergencies are both thought of and attended according to their potential in the future, is a practice that has been taken on recently by the British Fire and Rescue Service (FRS).

Anticipatory forms of governance rose to prominence in the FRS with the introduction of *The Fire and Rescue Services Act* in 2004 (Department for Communities and Local Government, 2004). The Act arose in response to suggestions made in the 2002 report *The Future of the Fire Service: Reducing Risk, Saving Lives* (2002) undertaken by Sir George Bain. The key recommendations of this report were that the FRS should be geared toward 'a new emphasis on the prevention of fire, rather than methods of dealing with fire after it has started' (10, 2004). This drive toward anticipating fires was to be achieved by developing 'a system of deploying people and equipment so they are prepared to deal with the most likely risks of fires in the most cost-efficient way based on risk management' (ibid). Shaped by the recommendations of the 2002 report, the *Fire and Rescue Services Act* introduced measures to ensure a risk-based approach to fire governance in Britain. The measures included formalising information collection procedures for FRSs across the country for the purpose of identifying risk. More autonomy, furthermore, was granted local authorities to decide how fire governance should be conducted in a way tailored towards the specific types of fire risks prevailing within local areas. In more recent years (Department for Communities and Local Government, 2008), a three pronged strategic approach to fire governance has been developed and adopted by many FRSs in Britain. This strategic approach is based primarily around modes of acting which are deployed before the moment of the fire itself and include preparedness, protection and prevention. The changes brought about demonstrate that the service now understand fire as a risk of the future. In turn, the organisational and strategic shape of the FRS is determined by what can be said about fire as a risk.

An abundance of literature across human geography and critical security studies asserts that the turn towards anticipatory modes of governance found in the FRS is a move mirrored across a wider apparatus of security organisations. Amongst others (Aradau and Van Munster, 2011), Amoore and de Goede (2008) observe for instance that risk governance procedures have become deeply

E-mail address: N.O'grady@soton.ac.uk

http://dx.doi.org/10.1016/j.geoforum.2015.06.015
0016-7185/

embedded within counter-terrorism whilst O'Malley (2010) has examined the application forms of anticipatory governance to more banal aspects of crime. Grove (2012), alternately, has interrogated the use of tactics of preemption in securing natural disasters deriving from climate change. Broad governmental pushes have sought to understand and govern disruptive events like terrorist attacks, natural disasters and crime by their potentiality, as events whose futures could be captured and acted upon in the present.

It is generally agreed furthermore that the enactment of anticipatory governance is in part reliant upon a variety of digital technologies. Surveillance technologies (Lyon, 2007; Murakami-Wood, 2007), new forms of calculation (Amoore, 2013), data circulation (de Goede, 2012) and organisational routines within which such technologies are embedded (Bigo, 2014) all feature as objects of inquiry in exploring how anticipatory governance is facilitated and conditioned through digital devices. An array of digital technologies is central also to the enactment of anticipatory governance in the FRS. A digital infrastructure has been constructed and has embedded itself at the heart of FRS operations. Following other work on the notion of infrastructure (Aradau, 2010; Starr, 1999), this digital infrastructure is not only composed of hardware, software, cables and code but as also encompassing both human analysts and multiple quotidian organisational processes. The digital infrastructure is composed thus of a range of non-human agents alongside human agents but also of different processes which allows this infrastructure to function. The infrastructure forms an assemblage of different material agents; the relations between which enable the generation of fire risk projections and inform strategic decision making on how fire can be governed before it unfolds as an event.

Drawing upon my research into the digital technologies operating in the FRS, this article contributes to the literature cited above by showing how digital technologies have renegotiated governance within an organisational context up to this point under-explored. Acting to articulate fire as a risk, the technologies found in the FRS contribute to an emergent set of governing practices found across an array of institutions, from financial tracking (de Goede, 2012) to border and airport security (Amoore and Hall, 2010; Adey, 2009; Salter, 2013). Digital security devices are harnessed within these organisational contexts to manage risks before their unfolding. Although remarking on entirely different cases, literature heretofore shows how such technologies enact governance of large scale events or security problems. In the literature cited above, research focuses on governing the next terrorist attack or the next natural disaster. Concentrating on fire governance, I show how digital technologies work also to render another event as a risk of the future.

The first contribution the article makes is to introduce a new organisational context and event to debates around anticipatory governance and digital security devices. The other contribution made is on a conceptual register. It is one which considers how digital security devices operate to envision future events and in turn legitimate and inform the enactment of anticipatory modes of governance. Previous literature has focused for instance on how renditions of the future are produced through the specific data mobilised in software (de Goede, 2012), how events are sensually or aesthetically rendered (Adey and Anderson, 2012; Collier, 2008; de Goede and Randalls, 2009) and forms of decision which guide the analytic process (Amoore, 2011, 2014). In this article, I examine how future events are envisaged and governed through what I call the interface performances configured and enacted within the FRS.

Interfaces account for the different relations which underpin the deployment of digital devices for security purposes. Expanding on pre-existing literature on interface (Galloway, 2012; Hookway, 2014) I argue that the notion of interface allows for a focus on the types of relations which are forged between human and non-human entities in digital processes. I demonstrate how interfaces are manifest in the spatial fixing of relations between human and the non-human whilst being relations that are also temporally coordinated. In addition, interfaces are affective encounters between human and non-human entities. I elaborate on the types of relations which interfaces enable through empirical material on organisational processes gathered through ethnographic observation of the FRS. Two organisational processes are concentrated on here: data sourcing and risk calculation. In regard to data sourcing, interfaces allow for an exploration of how the data harnessed for risk analysis result from spatially configured relations. I then turn to show how interfaces are crucial in facilitating different forms of calculation by engendering particular sensual and temporally fixed engagements between human and non-human agents. Overall, interfaces configure and perform relations between human and non-human agents and set these relations towards the singular trajectory of making sense of fire as a risk.

In the first section of this article, I outline and assess more deeply the notion interface as it appears in an emergent set of literature. Work on interface has instigated a process of conceptualising how digital practices are underpinned by human and non-human relations. Interfaces set trajectories for these relations whilst also being configured on spatial, temporal and affective registers. Based on ethnographic observation of the FRS digital infrastructure, the next two sections provide empirical material on how interfaces are performed. I consider the spatial configuration of data sourcing which facilitates fire risk calculations in section three. In the fourth section, I show how interfaces account for the relations performed between human and non-human agents in the process of risk analysis or risk calculation. In summarising the article in the conclusion, I argue that interfaces allow for focus on the types of relations between human and non-human agents which underpin the operation of security devices. I go on to show how this central argument of the article feeds into more broad discussion around issues of agency which emerge when examining digital security devices. Looking toward the future, I also intimate how thinking anticipatory governance through interfaces opens up new plateaus for change in the deployment of digital security devices.

2. The intervention of interface in relations between the human and non-human digital agents

Recent literature on digital technologies says much about the agential forces attributed to non-human technologies. Dodge and Kitchin (2005, 2011), for instance, have explored and analysed comprehensively the life of digital code in the production of spaces of everyday life. Using the example of bar-codes, the authors demonstrate how data are created, how data are selected according to different organisational ends and then processed through software to be transformed into information about the world. Although not explicitly aligned to it, this account of how digital entities conduct processes by which information is generated on the world is certainly emblematic of and resonant with work which speculates more widely on the effect of non-human digital entities on faculties previously reserved for humans. In his *The Language of New Media* (2001), Manovich demonstrates how digital technologies increasingly shape the conditions of possibility for knowledge creation. Manovich's argument follows a tradition in media studies which owes much to Friedrich Kittler and his inquiries into the linguistic systems which underpin contemporary computing. For Kittler, the algorithmic code through which computers work represent new 'discursive channel conditions' (2011,