Data, Interface, Security: Assembling Technologies that Govern the Future

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 occurrence. 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, deGoede, 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 (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 (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 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, 32) through which language is made operational. The generation of language and modes of thinking rely on self-perpetuating and auto-poetic computing systems. Studying these conditions, Kittler argues that knowledge creation and thought are capacities increasingly sequestered to the domain of computing and are thus obfuscated from human view and intervention.

The work cited above is highly influential and useful for exploring how processes of knowledge creation have been affected by developments in digital technologies since the second half of the twentieth century. However, concurrent work implies that this approach is too centred on the abilities of non-human digital entities and fails to cater for the continuing importance of human interventions in the deployment of digital technologies. Amoore's (2014) work, for instance, shows how, although increasingly operative through the gaze of ever more complicated algorithms, decisions on how to calculate futures are always inscribed with the intervention of human ingenuity. Following Levi-Bryant (2010), Ash (2013) has elaborated on the notion of allopoesis in describing the processes of communication technologies. Allopoesis is used by Ash to conceptualise how digital agents are involved in processes beyond their own functioning and, concurrently, how their functioning might be affected by the agency of other entities. Katherine Hayles (2005), alternately, distinguishes human cognition from its machinic equivalent of algorithmic processing of data,

arguing in turn that knowledge is performatively constructed through co-evolutionary dynamics established between the two.

In this paper, I contribute to work which attempts to situate the role of human agency in processes which also include the agency of digital technologies by elaborating on the notion of interface. The notion of interface is gaining increasing significance across disciplines (Ash, 2015, Drucker, 2011, Galloway, 2012, Hookway, 2014). For Galloway, interface expresses a threshold space wherein humans and non-human forces of computing relate to one another. As Galloway argues, interfaces mediate between the internal world of computing and the external world of human affairs. Interfaces exist in physical form such as computer screens and keyboards. But they also express the coming together of digital technologies within the wider social and historical contexts from which they emanate. So along with being present on the surface of the screen, Galloway uses the notion of interface to explore how new forms of subjectivity are constructed with the development of computing.

Galloway's understanding of interface is to be welcomed in how it begins to explore the embeddedness of human agency within digital processes. But his argument fails to engage thoroughly with the non-human agencies that characterise interface relations. Departing from Galloway, Brandon Hookway in his 2014 book entitled *Interface* seeks to ground his reading of the concept more in its disciplinary roots. Hookway shows that the notion of interface was coined in 19th century fluid dynamics. Here, interfaces were used to describe how lava and other fluids flowed through material environments and produced rock formations. Interface in this incarnation designated processes in which natural materials connected and encountered one another. In turn, interface was used to express what the results of meetings were for the environment in general. Grounded in its original use, Hookway goes on to use the notion of interface to conceptualise how the processes of digital technologies both instigate and rely on continuing intersections between human and non-human forces. Moments of interface account for the intersections between human

and non-human components which drive digital processes and what results from these relational processes.

But Hookway's account of interface also opens up the possibility of exploring the question of the agency that moments of interface themselves have. Interfaces relate the human and non-human to show how digital processes are instantiated but at the same time they have their own effect on the agencies they bring together. For Hookway then; 'The interface both defines a system and determines the means by which it may be known. It takes its place as the zone across which all activity must occur in order to possess meaning, force and power' (2014, 63). I propose that the agency of interface is apparent in how interfaces harness the different agential capacities of the human and non-human entities they bring together towards specific and singular governmental goals. In this paper, the singular goal interface orients towards is making sense of fire as a risk. As seen later, this goal is achieved through bringing human and non-human agents together to source data required for analysis and, later still, to perform risk calculation itself. The function of interface is thus to configure relations between human and non-human forces and, in the words of Bennett, to establish trajectories (2010, 31) for these related entities to pursue.

In this article, I develop the notion of interface to understand and analyse the ways in which situated interactions between human and non-human agencies enable processes through which the FRS makes sense of fire as a risk. Drawing on empirical material generated from ethnographic observation of FRS analysts, I focus on two organisational processes: data sourcing and risk calculation. Through empirical material on these processes, I contribute to literature on interface by showing that interfaces and the trajectories they enact take place on different registers. Interfaces take place through relations which are spatially fixed, temporally coordinated and which rely on sensual or affective encounters between the human and non-human. The spatial configuration and coordination of interface is evident in data sourcing practices to which I will turn to in section three. As a crucial entity for the enactment of risk based governance in the FRS, I show how data are

acquired and harnessed through spatial fixes between technologies, the movement of data and data ordering practices of human operators. Turning to calculation in the fourth section, interfaces take place with temporal and affective or sensual qualities. Data for instance which refer to past fire events are used to make future risk projections by being brought into interface with other forms of data, technology and human agents when calculation takes place. Intimately interwoven with the temporality of interfaces, calculation seeks to harness the imaginative capabilities of analysts in their relations to software in making fire risk projections. These different types of relations coordinate how different agents come together, and orient processes toward the trajectory of making risk projections.

3. Data sourcing and the spatial formation of interfaces

With the adoption of anticipatory modes of governance, the FRS has become reliant on a multitude of digitalised data. Data are used by the FRS to understand how fires start, what types of people are most vulnerable to fire and to discover what the consequences of fire have been and can be. It is primarily through data, in other words, that the FRS understands fire as an event. This data does not merely allow the FRS to understand fire as an event which has occurred in the past. Rather, the processing of data through a host calculative methods and analytic software means that fire can be articulated also as a risk of the future. Data are thus crucial to the FRS' capacity to understand fire as a risk and in turn develop governing strategies which intervene before fires take place.

But where does this data come from? Where are data, in other words, sourced? The answer is from a plethora of different sites. Data will be generated as a fire takes place in real time whilst also deriving from reflections on the tactics used to respond to fire. Data will be acquired moreover from commercial credit checking companies or investigations undertaken in fire incident locales where only ruined buildings now stand. The sites listed here are far from exhaustive but already intimate the vast, disparate collection of spaces used to source data.

But just to say that sites for data sourcing are disparate does not mean that sourcing itself is a completely incoherent and fragmented activity. Indeed, data sourcing is a process fixed and arranged within the FRS and across its multiple sites of operation. As I will show in this section, data sourcing is a process which relies on the formalised spatial configuration and coordination of different technologies, of different agential forces. It is a process, furthermore, which depends upon the regulation and ordering of data flows through space. The spatial configuration and enactment of data sourcing can be evidenced by a closer look at what is called the Incident Recording System (IRS). The IRS is the central depository for all data relating to past incidents that the FRS has attended. IRS has the capacity to collect up to 197 different variables on fires. The database can contain, for example, swathes of data on the time at which individual fires happen, how long it takes the FRS to arrive at the scene of a fire or the locations at which fires have occurred. It also collects data on who alerted the service to a fire, what forms of equipment were used and which personnel were present at the scene of an incident.

To source and capture data from the scene of incidents, IRS occupies and is configured across three distinct spaces. It exists primarily on desktop computers within the headquarters of the FRS. The role of IRS within FRS headquarters is as a central hub for all data recorded from the scene of an incident. It is in this site that all data will be collected. Once collected, as I will discuss in more depth below, human operators at this site will then distribute data to different analytic software the FRS uses to make risk calculations. But IRS is also present on tablets which fire fighters take to incident sites. At the scene of the incident itself, a multitude of data might be collected. Data accrued at the scene of an incident includes whether people were injured in the fire and, if so, how many. Fire fighters will record any obstructions to responding to a fire and what forms of protocol were deployed at the scene. Lastly, IRS is connected to and acquires data from FRS control rooms. Taking phone calls from the public and alerting the FRS to incidents, informing fire-fighters of traffic on routes to the scene and any adverse weather conditions, control rooms coordinate FRS response to fires from a distance. Control room operators hold a privileged position in regard to the sourcing of a number of different

data. They will record for example the time at which a fire was deemed to start or how long the FRS takes to arrive at an incident.

The spatial configuration of IRS across these three coordinated sites allows a multitude of data to be captured and harnessed by the FRS. But the configuration of data sourcing through IRS is not underpinned merely by static nodes across a variety of locales. Rather, the spatial configuration which engenders data sourcing relies on a coordination of movement too. To transfer data on a fire from the control room or from the incident site to the main IRS database in the FRS headquarters requires data circulation. What are called export and import functions operate and connect different sites and the multiple appendages of IRS to one another. These export and import functions are portals which connect IRS in its existence as a central database in the FRS headquarters to IRS branches and outposts both within the control room and at the scene of a fire. Export and import functions thus work to instigate and regulate the movement of data from different spaces to the space of the FRS headquarters.

IRS is a software which enables, performs and is itself enrolled within an interface process which exists across space. Material sites of the control room, the scene of an incident and the headquarters are spatially related to one another through import and export functions. These functions enable the circulation of data which, upon arrival in FRS headquarters, interface with one another as data on a specific fire incident. Upon the arrival of data, however, human operators are absorbed and enrolled within the interface which is enacted in the process of data sourcing. The role of human operators is to sift data into different categories within the IRS database to ensure, for example, that data relating to the time of an incident is stored with other data on this variable. The contribution by human analysts to the interface is one of ordering the data sourced for its future use across the FRS digital infrastructure.

It is in this ordering practice that trajectories are set through the interfaces performed between humans and data of different forms. In the case of data sourcing, the trajectory established concerns

where data gathered will be circulated to within the digital infrastructure it now inhabits. By ordering data into different categories, human analysts determine to what databases data will travel. Data on the time of fires will be moved for instance to software which seeks to identify and track changes in trends which trace fire by the time of its occurrence. By combining data with the ordering practices of human analysts, the interface performance taking place can operationalise data within specific software packages whose analysis serves to render fire as a risk of the future.

Data sourcing practices in the FRS are reliant on spatial fixes and configurations between a variety of different technologies in the FRS digital infrastructure. Bringing data into the FRS, these spatial relations are based on, configure and enable interface performances. Circulated through IRS import functions into the FRS headquarters, data are brought into interface with one another. The interface which takes place within the FRS headquarters is not, however, confined only to data and software. Rather, human operators are enrolled within the interface performance. The interface performed here between human, IRS software and data acquired is one which makes data function for the specific purpose of risk identification. Through the ordering practices described above, interfaces set the trajectory of data circulation once data have arrived in the FRS headquarters. This interface dictates where data goes, what software it will come to inhabit and how, in turn, data will be used to articulate fire as a risk. Even at the preliminary stage of data sourcing then, important interfaces can be revealed which orient human and non-human relations towards the identification of fire risk. In the next section of this article, I describe in-depth what happens to data once it has been circulated to specific software packages. Specifically, I explore how data are drawn upon and subjected to modes of calculation to articulate fire as a risk of the future.

4. Risk Calculation as a performance of interface

To implement and practice forms of anticipatory governance the FRS needs to understand fire as an event by its potential to occur in the future. In other words, fire must be articulated, measured and detected as a risk. A number of calculative methods have been developed and actioned through

software packages in the FRS digital infrastructure to know fire as a risk. Acquired from the interface performances involved in sourcing described above, data on the time at which previous fire incidents have taken place will be collected and used to suggest the time at which future fires might occur. In another calculative process, data containing the geographical coordinates of past fires will be uploaded on to databases and will interface with data on the spatial distribution of lifestyle groups on a map. This form of risk mapping will be used to attempt to reveal what specific lifestyle groups are most vulnerable to fires.

Not only are these forms of calculation facilitated through the collection of data and data sourcing methods described in depth above. Rather they rely on the acquisition and deployment of a variety of commercially available software alongside software that has been specifically designed for the FRS. Of the latter, what are called 'bespoke' software; analysts in the FRS have developed for instance their own risk matrix programme which charts correlations between fire incidents and different variables such as time of day, location and consequence on an Excel spreadsheet. On the other side of the spectrum, substantial fees have been paid by the FRS to acquire the MOSAIC lifestyle analysis database provided by the credit checking company Experian. Generated through analysis of consumption and credit data garnered from credit card usage, internet tracking devices and consumer surveys, the MOSAIC database supplies the FRS with lifestyle classifications for the local population which the FRS governs. As a commercially available database, MOSAIC will be tailored toward highlighting those lifestyles most vulnerable to fire.

Different forms of calculation and analysis by which fire is known as a risk will be aligned to and used to inform specific governing strategies used to intervene on fire risk. Depending on what software data are processed through, fire risk is made into an object of security in different ways which call forth particular strategies for governing fire risk. Acting to highlight those lifestyle groups most vulnerable to fire risk, the MOSAIC software will facilitate and condition decision making which enacts prevention strategy in the FRS. Prevention strategy, which amounts to visiting domestic

properties to ensure fire safety mechanisms like smoke alarms are installed, will be targeted to those lifestyle groups MOSAIC considers vulnerable.

The picture painted of calculation performances in the FRS thus far would suggest a Kittlerian (1986) form of post-technocratic governance in which non-human computer-based technologies dictate security decisions. The only interface performance in this model would be between forms of data and the hardware, software and fibre-optic cables they temporarily inhabit in generating fire risk projections. However, my ethnographic observation of calculative processes and performances in the FRS reveals such a picture to be fallacious. Human analysts are harnessed within, and crucial to, calculative processes taking place in the FRS. Their enrolment is evident in the moments and experiences of interface which are configured and performed in the calculative process. That is, human enrolment in the calculative processes which articulate fire as a risk are evident in forms of interface whose relations are sensually and temporally based.

Rather than casting the agency of human analysts into the shadows, the digital technologies which have risen to prominence in the context of security rely on relations to humans in new ways. By investigating the interfaces which take place, I will show how calculative processes are coordinated and performed by two forms of relations between human and non-human agents. Facilitating modes of calculation, relations between human and non-human agents operate temporally to transform data on past fires into data on fire risk. Calculation, furthermore, functions through harnessing sensual ties between the human and non-human. In particular, the imagination of human analysts must be enrolled into processes of calculation. Taking place on temporal and sensual registers, the interfaces performed pursue a specific trajectory of articulating fire as a risk.

4 i) Interfaces which change the temporal address of data

The data which are sourced, which circulates and which are mobilised in the FRS have specific temporal features. Data derive from and designate specific events which unfolded in time. Data in

the FRS can thus be said to have a particular temporal address. Drawing on the last section, it is evident that much of the data sourced by the FRS addresses past fire incidents. In its insertion into the FRS digital infrastructure, data which initially has a temporal address to the past will be circulated to and deployed within different databases for different purposes. For instance, data on previous fire incidents will be transported seamlessly into performance monitoring software which records the conduct of fire-fighters when responding to fires. Where this data will be used to inform risk analysis, its deployment and harnessing becomes a more complicated process. The data, of course, must be mobilised in risk analysis to make projections of future fires. The temporal address of the data must thus be transformed from past reference to future reference.

This temporal shift in the reference of data takes place through different interfaces configured between and performed by different agents. Both human and non-human agents are enrolled within the interfaces performed. The risk profiling and vulnerability targeting undertaken through the above named MOSAIC software exemplifies this interface taking place on a temporal register. As documented above, MOSAIC undertakes analysis of lifestyles across Britain. It draws on 'over 440 data elements' (2009, 13) such as the British Household Survey, Electoral roll, self-reported lifestyle surveys and smart recording technologies which monitor the movement of over eight million Britons across the internet to come up with fifteen lifestyle groups said to prevail across Britain. On its arrival in the FRS, MOSAIC is used to undertake an analysis of the lifestyles prevailing across the region in which the FRS operates to show those lifestyles most vulnerable to fire risk. The Incident Recording System (IRS) uses export functions to feed data into MOSAIC. The kinds of data circulated to MOSAIC from IRS are multiple and heterogeneous. One of the most important forms of data sourced from IRD for the analysis that MOSAIC will undertake is data on the geographical location of fire. Once deposited, this data are uploaded into a Geographic Information Systems (GIS) component inbuilt in MOSAIC. The GIS component contains a map into which data on the geographical coordinates of each fire over the last three years are uploaded. As the GIS component processes the fire coordinate data, locations of fire overlap on the map. Clusters of fire incidents form within

different locations of the map designating 'hot-spots' for previous fire occurrence. The map MOSAIC presents at this stage only shows where fires have occurred in the past. The temporal address of data acquired from IRS still refers to the past.

To shift the temporal address of data toward the future, fire location data are brought into interface with other data on the spatial distribution of different types of lifestyle groups across the map. MOSAIC superimposes another data-set on to map and, as such, the interface takes place visually on the map. Showing fire distribution and lifestyle group dispersal, the map allows correlative calculations to take place. Most importantly, the map allows analysts to perceive which lifestyle groups are most vulnerable to fire according to which groups inhabit those spaces in which fires are most frequent. At the time of writing, the lifestyle group most vulnerable to fire is known as group K. Although divided into sub-categories, this group is described by Experian overall as 'Residents with sufficient incomes in right to buy council houses' (2009, 14) who tend to live in areas where there is 'very little anti-social behaviour' (ibid). As opposed to 'well educated' this group is made of 'people who are practical and enterprising' (ibid), who value 'self reliance and responsibility' (ibid). This group is often frequently invested in 'informal community networks, often centred around family and former school friends '(ibid)which are re-enforced over time by entertainment such as 'Television and the Home computer' (ibid).

In establishing the grounds for correlative calculation and identifying lifestyle groups considered most vulnerable to fire, the temporal address of fire location data within the map is no longer strictly toward the past. Fire location data interfaces with lifestyle distribution data to envision and produce claims about the potential for fire in the future. Through its interface with the MOSAIC database and lifestyle data, fire location data changes in its temporal address; from speaking merely to the past to being enrolled in analytic processes which seek to make sense of the future. Risk calculation in the FRS is thus facilitated by a performance of interface between different forms of data and software. This interface re-mobilises historical data towards generating accounts of the potential future.

Human analysts are also vital to the interface performances which underpin and organise risk calculation here. The interjection of humans and their enrolment within this form of interface is most obvious where faults and problems are found in the risk analysis that MOSAIC undertakes. In establishing correlations between clusters of previous fire locations and lifestyle group dispersal, I observed a problem in the analysis. Rather than fitting neatly into areas specific lifestyle groups were believed to inhabit, fire location clusters overlapped and exceeded these areas. As such, the mapping undertaken did not give a clear sign of which lifestyle groups are most vulnerable to fire risk. With this ambiguity noted, the enrolment of humans into the interface performed shows its importance. Viewing the risk map generated by MOSAIC, analysts will make decisions concerning which lifestyle group the risk distribution reveals as vulnerable. They do so through gauging which lifestyle groups occupy the most of the space in which clusters of fires can be found. The interjection or enrolment of human analysts into calculative interface performances is thus pivotal to the functioning of MOSAIC overall. Rather than being fundamental to generating renditions of the future through data which refers to the past, human analysts adjudicate, validate and verify the risk projections made. The human intervention is thus to steer analysis to one rendition of the future over another. In relationship with MOSAIC software, human analysts play an important role in setting the trajectory of risk calculation towards a specific understanding of the future. The trajectory in this case concerns what kinds of lifestyle are deemed most vulnerable to fire risk. Once human analysts have intervened in this way, MOSAIC analysis will go onto inform strategic decision making on where and to whom preventative resources should be targeted.

The effect human analysts have on risk calculation is to influence what rendition of the future prevails and in turn how this vision of the future informs strategic decision making in the here and now. The form of interface which underpins calculation here is based on temporal issues. Different agents of the FRS digital infrastructure enact relations to transform data on the past into visions of the future. As I will now turn to show, however, the process of risk calculation is underpinned by interfaces which mobilise human and non-human agents in other ways.

4 ii) The enrolment of human sense into interfaces

The intervention of human analysts in MOSAIC comes once risk projections have been made by the relations between data and software. Humans are enrolled in the interfaces taking place here as adjudicators or verifiers. In other instances of risk calculation, human analysts are enrolled in interfaces at more preliminary stages in the process of calculation. Where this is the case sensual relations between human and non-human agents of the digital infrastructure are integral to articulating fire as a risk. The case of the Fire Service Emergency Cover Toolkit or FSEC exemplifies the integral status of human sense within interfaces which underpin analysis in the FRS. FSEC was implemented in the FRS digital infrastructure in 2004, the same year as the *Fire and Rescue Service Act* (2004) which crystallised the risk governance rationale under which the contemporary FRS operates. Through the analysis it undertakes, FSEC seeks to transform FRS response strategy into an element of anticipatory governance. This is achieved by analysis which seeks to discover the FRS' quickest possible response time to fires by assessing the relation between the geographical distribution of FRS resources and the spatial distribution of fire risk. By concentrating on the resources at their disposal and how such resources might arrive at the scene of fires quicker in the future, the FRS has made response a strategy which can be prepared for in advance of fire. FSEC seeks to discover the optimal location of resources according to the most frequent locations for fire. As a result FSEC can inform strategic decision making on where resources might be best placed to shorten response times for future fires.

FSEC is a risk mapping technology which, similar to MOSAIC, has an GIS application in-built. The map that FSEC presents includes Ordinance Survey data on terrain, points of elevation, buildings of significance and population density for instance. It also envisions travel data on road networks, speed limits, traffic congestion times and ulterior transit routes like bridges and rivers. Superimposed onto the surface of this map are data on the geographic coordinates of every fire incident in the last three years and the location of FRS resources used to respond to fires are then

uploaded on to the map. Fire location coordinates appear as flame symbols. Over time these symbols gradually cluster and overlap as incidents with overlapping coordinates appear. The location of resources is indicated by red dots which appear across the map.

Fire risk is derived from bringing into interface and analysing the reciprocal relationship between two forms of data: previous fire distribution and resource allocation. FSEC does this by automatically running what is called a time-travel matrix analysis. Using resource location as a starting point, FSEC simulates the time it would take the FRS to arrive at each fire incident. The time travel-matrix calculates response times according to a number of variables. These variables include the distance from resource to incident location, average traffic congestion at the time of an incident and the effect points of elevation and the use of bridges have on the speed at which fire engines can travel. On the basis of this calculation, FSEC calculates what is called the Base-Case of all response times across map. This Base-Case shows the normal time it takes the FRS to arrive at each fire from the closest resource. Running this analysis changes the temporal address of data on fire location. As the time-travel matrix shows normal response times, it is held that response times for fires should persist in the future so long as the location of resources are not changed. As such FSEC shows the distribution of fire risk across different regions in the map according to how long the service takes to arrive at different areas. Fire risk distribution is shown by colour coding the map, with red areas being the highest risk, areas coloured turquoise being of intermediate risk and yellow being the lowest risk.

Up to this point, calculation processes take place according to interfaces between data which is enrolled within FSEC software. Nevertheless to enhance response times and become prepared for future fire emergencies human sense must be harnessed and enrolled within the calculative process. The particular human sense harnessed in FSEC is imagination. Human imagination is enrolled within the interface in a way structured through the specific calculative logic by which FSEC, once the initial risk map is established, comes to operate: hypothesis. Human analysts will assess the fire risk

distribution visualised on the map and in turn use their imagination to think of new hypothetical locations for FRS resources. Analysts will then manually re-write the geographical coordinates of FRS resources on the map. Once analysts have done this, FSEC is made to re-run time-travel matrix calculations to gauge the effects of resource reallocation on the distribution of fire risk. The relation between human analysts interfacing with FSEC is iterative here. Analysts' imagination will be harnessed in hypothetically reconfiguring the location of resources over and again. Each time, fire risk will shift and transform in its distribution across space. The relation between analyst and FSEC will continue until the map shows risk distribution which analysts consider optimal.

In the case of FSEC risk mapping human interface is crucial to the performance of calculation. Human sense is required in making decisions as to where resources should be allocated and relocated in undertaking this iterative analysis. Based on hypothetically relocating resources, the functioning of FSEC relies on the enrolment of human imagination into the interfaces underpinning calculation. The interface performed here is oriented toward a specific trajectory too; that of identifying fire risk in relation to resource location. But the calculative processes performed at the interface, just as with MOSAIC, also serve to inform strategic decisions. In the case of FSEC, these decisions implement response preparedness in the FRS. The analysis undertaken and projections generated by FSEC shape what are called response standards. Response standards articulate FRS expectations on the time it will take to arrive at the scene of an incident. In consultation documents for their *Integrated Risk Management Plan* of 2014-15, the FRS I studied state that their response standards are 'to attend 70% of house fires within 8 minutes and 90% within 11 minutes' (2014, 22). Articulated through standards or expectations, response strategy in the FRS is made into an element of preparedness. Acting as expectations for the performance of the FRS, these response standards seek to guarantee the mobilisation and arrival of the FRS in a specified time frame for future incidents.

5. Conclusion: Changing the way we interface

The reproblematisation of fire governance operations in Britain has been primarily organised around a new understanding of fire as an object of security. A dominant understanding of fire prevailing in the FRS, as the article has evidenced, is as an event that not only sparks spontaneously in the present but is a risk of the future to come. This renegotiation of the understanding of fire as an event has worked to legitimate and engender modes of anticipatory action and intervention which have already been traced in their deployment across a vast set of security organisations (Amoore, 2013, Adey, 2009, Adey and Anderson, 2012, Aradau and Van Munster, 2012, Bonelli and Ragazzi, 2014, de Goede, 2012).

But what underpins the enactment of these modes of anticipatory governance in the FRS are a set of processes, of materials, of entities which collectively work to generate fire risk projections. Composed of data, software, hardware, humans and organisational processes, the digital infrastructure of the FRS envisions and supplies accounts of potential fire events. These relations have been conceptualised through the notion of interface in this paper. I have argued that interfaces offer a way to conceptualise the relations configured and performed between materially heterogeneous agents enrolled in the process of identifying fire as a risk. The relations found in sites, moments and experiences of interface enable processes by which fire risk projections are made. My research shows that interface is fundamental to the acquisition of data and its mobilisation towards specific software. At the same time, interfaces underpin calculation practices by which risk projections are made. Fundamental to both data sourcing and risk calculation, interfaces play a crucial role in establishing governmental trajectories for relations established between the human and non-human. The trajectory established is one oriented toward the identification of fire as a risk which, in turn, shapes and legitimates strategic intervention on fire incidents before they occur.

In examining interface this article contributes to existing literature by claiming that, and conceptualising how, security devices operate through configuring relations between their component parts. I have used the notion of interface to take a more in-depth look at the question of

relationality in regard to the operation of security devices. Specifically, I have inquired into the types of relations found within interfaces. I have shown, for instance, that interfaces can be used to explore how data sourcing relies on spatial configurations between human and non-human entities. In the process of risk calculation, alternately, relations are coordinated and practiced around temporal issues and by enrolling the sensual qualities of human analysts into relations with other digital, non-human agents. The notion of interface opens up for consideration how human and non-human agents relate, the trajectory towards which these relations are oriented and the types of relationships which underpin interface.

What has pre-ceded allows for two wider claims about the politics of interfaces and digital security devices in finishing this article. Firstly, interfaces open up to inquiry how security devices operate through the harnessing and deployment of human and non-human actants' agency in particular ways. Through the interfaces explored in this paper, the FRS have been able to collect data for risk analysis, data referring to the past has been re-oriented towards the future and hypothetical forms of analysis have been deployed where they were never found before. Interfaces contribute to the conditions which afford the FRS the possibility of taking a risk based or anticipatory approach to fire governance. Interfaces do so by enacting specific spatial relations between different components of the digital infrastructure. Interfaces, furthermore, gather agents together to solve temporal issues relating to data whilst bringing human imagination into the process of calculation also. Through interface, the agency of infrastructural components can be harnessed in different ways and explored according to the types of relations which prevail within interfaces.

The second wider claim relates to how the notion of interface allows for an appraisal of how digital security devices might be changed in their deployment and the effects of this deployment. At the same time as questioning how risk identification is achieved through harnessing the agency of human and non-human agents, interfaces open up to discussion how practices might be differently undertaken if relations between components in the digital infrastructure were made and configured

in alternate ways. Although no empirical evidence can of course be supplied for this claim at the moment, one could speculate on how the interface performances discussed in the article could be reconfigured. If data other than that referring to lifestyle groups in MOSAIC was enrolled in calculative interfaces, for instance, how would the FRS understanding of vulnerability change? Understandings of vulnerability could be renegotiated if age data, which is understood to bear a relation to fire outbreak[1], replaced lifestyle data as the primary variable for calculating who is vulnerable to fire. What if, instead of just a means to hypothetically rewrite the geographical coordinates of resources, human imagination was enrolled into other calculative processes? Could imagination be used to curtail risk projections that are not likely to happen and whose impact may be only in the risk perceptions they induce in subjects of governance rather than the occurrence of an event itself? Interfaces, at the same time opening up to inquiry the processes underpinning governance, are about relational configuration. Points of change to how security devices are performed and enacted can appear where questions are asked about how the relations underpinning such devices might be reconfigured and thus re-deployed.

References

- Adey P (2009) Facing Airport Security: Affect, Bio-politics and the Pre-emptive Securitisation of the Mobile Body, Environment and Planning D: Society and Space, Volume 27, Issue 2, p 274-295
- Adey P and Anderson B (2012) Governing Events and Life: Emergency in UK Civil Contingencies, Political Geography, Volume 31, p24-33
- Adey P and Anderson B (2011) Affect and Security: Exercising Emergency in UK Civil Contingencies, Environment and Planning D: Society and Space, Volume 29, pp1092-1109
- Amoore L (2009b)Lines of Sight: On the Visualisation of Unknown Futures, Citizenship Studies, Volume 13, Number 1, pp17-30

[1] As evidenced whilst undertaking ethnographic observation of FRS analysts 09/2011

- Amoore L (2011) Data Derivatives On the Emergence of a Security Risk Calculus for our Times, Theory Culture Society, Volume 28, 24-43
- Amoore L (2013) The Politics of Possibility: Risk and Security Beyond Probability, Duke University Press, Durham
- Amoore L (2014) Security and the Incalculable, Security Dialogue, Volume 45, pp 243-249
- Amoore L and Hall A (2010) Border Theatre: on the Arts of Security and Resistance, Cultural Geographies, Volume 17, Issue 3, pp 299-319
- Anderson B (2010) Security and the Future: Anticipating the Event of Terror, Geoforum, Volume 41, Issue 2, pp227-235
- Aradau C (2010) Security That Matters: Critical Infrastructure and Objects of Protection, Security Dialogue, Volume 41, Issue 5, pp 491-514
- Aradau C and Van Munster R (2011) Politics of Catastrophe: Genealogies of the Unknown, London, Routledge
- Ash J (2013) Rethinking Affective Atmospheres: Technology, Perturbation and Space times of the Non-Human, Geoforum, Volume 49, p20-28
- Ash J (2015) The Interface Envelope: Gaming, Technology, Power, Bloomsbury, New York
- Barclay C (2004) The Fire and Rescue Services Bill, House of Commons Library, London
- Bennet J (2010) Vibrant Matter: A Political Ecology of Things, Duke University Press, Durham
- Bigo D (2014) The Insecuritization Practices of the Three Universes of EU Border Control: Military/Navy- Border Guards/Police- Database Analysts, Security Dialogue, Volume 45, Number 3, pp209-225
- Bonelli L and Ragazzi F (2014) Low-Tech Security: Files, Notes, Memos as Technologies of Anticipation, Security Dialogue, Volume 45, Issue 5, pp476-493
- Bryant L (2011) The Democracy of Objects, Open Humanities Press,
- Collier SJ (2008) Enacting Catastrophe; Preparedness, insurance, Budgetary Rationalization, Economy and Society, Volume 37, Issue 2, pp224-250

- Communities and Local Government (2008), Fire and Rescue Service National Framework 2008-11
- County Durham and Darlington Fire and Rescue Service (2014), Integrated Risk Management Plan Consultation 2014-15
- de Goede M (2008) Beyond Risk: Pre-mediation and the Post 9/11 Imagination, Security Dialogue, Volume 39, Issue 2-3, pp 155-76
- de Goede M and Randalls S (2009) Precaution, Preemption: Arts and Technologies of the actionable Future, Environment and Planning D: Society and Space, Volume 27, Issue 5, pp859-878
- de Goede M (2012) Speculative Security: The Politics of Pursuing Terrorist Monies, University of Minnesota Press, London
- Department for Communities and Local Government (2004) Fire and Rescue Services Act
- Dodge M and Kitchin R (2011) Code/Space: Software and Everyday Life, MIT Press, Cambridge
- Dodge M and Kitchin R (2005) Codes of Life: Identification Codes and the Machine Readable World, Environment and Planning D: Society and Space, Volume 23, pp851-881
- Drucker J (2011) Humanities Approaches to Interface Theory, Culture Machine, Volume 12, pp1-20
- Experian Limited (2009) Improved Outcomes through Applied customer Insight; Experian's MOSAIC Public Sector Citizen Classification for the United Kingdom
- Galloway A (2012) The Interface Effect, Polity Press, London
- Grove K (2012) Pre-empting the Next Disaster: Catastrophe Insurance and the Financialization of Disaster Management, Security Dialogue, Volume 2, Issue 43, pp139-155
- Harman G (2009) The Prince of Networks: Bruno Latour and Metaphysics, Re:press, Melbourne
- Hookway B (2014) Interface, The MIT Press, Cambridge

- Kittler F (1986) Gramophone, Film, Typewriter, Brinkman and Bose, Berlin
- Latour B (2005) Reassembling the Social: An Introduction to Actor Network Theory, University of Oxford Press, Oxford
- Lobo-Guerrero L (2011) Insuring Security: Bio-politics, Security and Risk, Routledge, London
- Lyon D (2007) Surveillance Studies: An Overview, Polity Press, London
- Manovich L (2001) The Language of New Media, MIT Press, Cambridge
- Murakami-Wood D Beyond the Panopticon: Foucault and Surveillance Studies in Elden S and Crampton J (2007) Space, Knowledge and Power: Foucault and Geography, Ashgate, Aldershot
- O'Malley, P (2010) Crime and Risk, SAGE, London
- Salter M To Make Move and Let Stop: Mobility and the Assemblage of Circulation, Mobilities, Volume 8, Issue 1, pp 7-19, 2013
- Starr SL (1999) The Ethnology of Infrastructure, American Behavioural Scientist, Volume 43, Number 3, pp377-91
- Winthrop-Young G (2011) Kittler and the Media, Polity Press, Cambridge