

Critical Infrastructures and the Biopolitics of Resilience

By: Christopher Zebrowski
PhD Candidate Keele University

Paper presented to SGIR Conference
Stockholm, Sweden
September 11, 2010

Work in progress, please do not cite without the permission of the author

(5,980 words)

Abstract:

Critical Infrastructure Protection (CIP) has been identified as a priority in optimizing the resilience of the United Kingdom to various contingencies. Of these infrastructures, a resilient telecommunications grid is recognized as the most 'critical' of critical infrastructures. This paper will begin by discussing the integral role information circulation plays in the planning and exercising of self-emergent emergency responses coordinated by the UK Civil Contingencies Secretariat. Locating the priority placed on 'informational superiority' in its capacity to translate into 'decisional superiority' this paper will look beyond the technological solutions prioritized in resilience literatures (c.f. Arsenault and Sood, 2007, Gorman, 2005) and focus on the governance of emergency responders within these operations. How are processes of decision-making understood within these operations? How are these processes being optimized? What are the consequences for the way we understand agency and 'govern through freedom' (Rose, 1999)? In asking how individuals are governed, so as to exacerbate critical circulations, this paper aims to problematise the relationship between humans and critical infrastructures by drawing attention to the extent to which individuals need to be secured in order to optimize the functioning of technologies said to provide the conditions for their freedom. The conclusion of this paper will look to draw out the consequences of these insights for understanding contemporary practices of neo-liberal governance.

Between the 16th and 21st of February 2007, a full national preparedness exercise entitled Winter Willow was coordinated by the United Kingdom's Civil Contingencies Committee to test the local, regional and national response to a pandemic flu. Incorporating over 5000 participants from government, industry and the volunteer sector the exercise was the largest of its kind to be performed within the UK. The scenario simulated a UK alert level of 4 (widespread cases within the UK) in order to exercise decision-making processes within governmental agencies and test the capacity for a wide range of governmental and non-governmental organizations to coordinate an effective and speedy response to an emergency. Stated objectives of Winter Willow included "test[ing] information flows, real-time modelling and access to timely expert advice during a pandemic" (Government Office for the South East, 2007) and the follow-up report stressed amongst the 'lessons learned' the need to streamline communication channels and consistency in reporting templates (UK Resilience, 2007).

These 'lessons learned' reflect the concerns of previous exercises aimed not only at improving inter-agency communication but also the ability of "all organizations to assimilate information quickly enough to inform the necessary decisions" (Environment Agency, 2005). Ensuring that the informational superiority afforded by information and communications technologies (ICT) translates into decisional superiority has emerged as a problematic within the time-sensitive arena of emergency preparedness and response planning. This paper will examine the ways in which subjects are being governed to ensure that informational technologies translate into accelerated decision-making within the preparedness exercises organized by the United Kingdom's Civil Contingencies Secretariat (CCS): the Home Office department responsible for enhancing 'UK Resilience'. It does so by examining

preparedness exercises as a technology of governance aiming to accelerate emergency responses.

Preparedness exercises are a principle technology for testing, training and optimizing emergency responses in the United Kingdom and, as such, they deserve attention in their own right. This paper will examine the forms of subjectivity currently valorized within these exercises through an analysis of the practices of governance which seek to fashion them. Specifically it focuses on practices of government which look to improve the capacity of actors and departmental agencies to quickly sort and process the influx of information available to them to arrive at decisions quickly. However, this paper also takes exercises to be sites of experimentation, in which emergent practices of governance aiming to engender 'resilience' can be trailed, tested and optimized before transfer to more general applications of improving 'UK resilience' (in much the same way that the colonies were formerly utilized). An analysis of preparedness exercises would therefore contribute to an analytical apparatus for studying the rationalities and technologies of governance including, but not limited to, those directed towards optimizing 'UK resilience'. The conclusion of this paper will attempt to sketch an outline for such a study.

Communicating Resilience, Optimizing Emergence

Before pressing on, we should remind ourselves that this is not the first time that communications have appeared as a problematic site for the organization of emergency responses. Historically, however, the opposite problem was often encountered: from the very beginnings of British Civil Defence, with establishment of

the Air Raids Precaution (A.R.P.) Committee in 1921, to the Civil Defence plans of the Cold War information circulation during an emergency was problematised by fears of inducing public panic. O'Brien accounts how early civil defence plans drawn up by the A.R.P. consolidated around a problematic which pitted the democratic freedom of information against the potential devastation that public panic itself would pose in the midst of a German Luftwaffe attack (O'Brien, 1955). The A.R.P.'s decision to limit intelligence of impending attacks to emergency personnel, while adopting a disciplinary framework to control panic based on Regional Commissioners (which had been originally constructed for strike-breaking purposes) is testament to the powerful hold public panic exerted over emergency planning. Grant, in his study of British Cold War Civil Defence, documents how public panic continued to exert an influence over civil defence planning through the Cold War (Grant, 2010).

It is curious then that by the 1980's 'disaster researchers'—a burgeoning field of research with disciplinary aspirations—were proclaiming panic a 'myth' (cf. Sime, 1983, Quarantelli and Dynes, 1972, Quarantelli, 1977, Keating, 1982). Basing their conclusions on a sizeable collection of empirical case studies,¹ disaster researchers proclaimed that in stark contrast to the competitive, self-interested behaviour assumed to manifest within emergency situations empirical research suggested that cooperation, even altruism, was far more common. To the extent that panic was said to be witnessed, researchers claimed, in retrospect, this was better explained as rational decision-making based on limited, or false, information which gave onlookers the impression of erratic or even 'irrational' behaviour. The persistence of the 'myth' of panic, they warned, could in fact be counter-productive—encouraging authority

¹ Cf. The E.L. Quarantelli Resource Collection at the University of Delaware's Disaster Research Centre (DRC) (<http://www.udel.edu/DRC/E.L.%20Quarantelli%20Resource%20Collection/index.html>)

figures to withhold the information in the onset of an emergency upon which participants could begin to organize their own rescue and response.²

Resilience strategies in emergency preparedness and response are premised on providing technological solutions to extend the ‘natural’ abilities of social collectivities to self-organize in a response to crisis. As such, resilience discourses are steeped in the language of the ‘freedom’, understood as less governance, through technological and system-design solutions (Cf. Gorman, 2005, Allenby and Fink, 2005, Arsenault and Sood, 2007). But the contemporary problematic of ‘ensuring informational superiority translates into decisional superiority’ within preparedness exercises shows that subjects must also be train-into these technologies. Governance, while perhaps less prevalent in the midst of an emergency itself, shifts its emphasis to the pre-event phase: aiming to nurture and promote ‘resilient’ subjectivities

Since its inception in 2001, the Civil Contingencies Secretariat (CCS) has echoed this emphasis on communications within its strategy of optimizing ‘UK resilience’ to a range of unanticipated disruptions. A resilient, and thus reliable, telecommunications infrastructure has been prioritized as a “fundamental enabler underpinning the effective response to any emergency”.³ Initiatives to create resilient communications infrastructure for emergency responders and government include the development of the High Integrity Telecommunications System (HITS), the Mobile Telecoms Privileged Access Scheme (MTPAS), and the National Resilience Extranet (NRE) which, when taken together, comprise a layered communications infrastructures providing built-in redundancy in the event of disruption. The CCS has

² The endurance of the myth ‘panic’ continues to exert a considerable hold on the general population as well as emergency-responders as noted within the Civil Contingencies Secretariat’s recently commissioned study, ‘*Understanding Crowd Behaviours*’ (2009) available at http://www.cabinetoffice.gov.uk/epcollege/news/understanding_crowd_behaviours.aspx

³ ‘Introduction to Resilient Communications’ *UK Resilience website*, http://www.cabinetoffice.gov.uk/ukresilience/preparedness/resilient_telecommunications.aspx

also sought to facilitate information sharing and emergency coordination between government and members of the telecommunications industry through the development of the National Emergency Alert for Telecommunications (NEAT) protocol, which was recently tested in Exercise White Noise led by the Department of Business Innovation and Skills with assistance from the CCS. Furthermore, UK Resilience, the official website of the CCS, provides a platform for the dissemination of a broad range of materials for emergency planners, industry and the public on preparing for emergencies. Regional Resilience offices likewise maintain preparedness websites, supplemented by mailing lists, which keep the public informed as to potentially disruptive challenges in the region, as well as the ongoing efforts of their regional offices to combat them.

Bruce Mann, Head of the Civil Contingencies Secretariat, describes resilience as “the ability to respond to an emergency, minimise and absorb any damage, and recover” (Mann, 2007). Enhancing resilience involves mitigating vulnerability and optimizing the capacity to not only endure crisis, but to ‘bounce-back’ from a potentially catastrophic event. For Lentzos and Rose resilience thus implies “a systematic, widespread, organizational, structural and personal strengthening of subjective and material arrangements so as to be better able to anticipate and tolerate disturbances in complex worlds without collapse, to withstand shocks, and to rebuild as necessary” (Lentzos and Rose, 2009: 243).

Resilience operates within a risk-based understanding of security (Zebrowski, 2009) in which ‘security’ refers to the mitigation of vulnerability rather than the absence of threat (cf. Aradau et al., 2008, Lobo-Guerrero, 2010) and, as such, should be situated within a broader trend in security discourses towards risk-based technologies associated with the framing of the contemporary security ‘environment’

in terms of the radical uncertainty of threats (Cooper, 2010, Dillon, 2007, Massumi, 2009). The discourse of radical uncertainty refers to the rapid emergence of dangers which exhaust predictive capacities such as terrorist strikes, the spread of epidemics, financial crises and natural disasters. Associated with this discourse is a new ontology of the emergency event: no longer characterized in legal-theological terms as the punctuated arrival of a Schmittian 'exception' to a pre-existing order, but in terms of an emergence (Dillon, 2007). The emergent ontology of the contemporary emergency event places emphasis on the *speed*, or rather the *acceleration*, of their becoming-dangerous as what is so radically threatening.

This particular framing of the contemporary security environment has been studied in relation to the emergence of strategies of pre-emption (Cooper, 2006, De Goede and Randalls, 2009) and the associated proliferation of surveillance and biometric technologies (Adey, 2009, Muller, 2008). Resilience operates according to a related, albeit inverted, logic to that of pre-emption: whereas pre-emption seeks to detect and terminate *potential* threats before they become dangerous, resilience looks to optimize the conditions of emergence, or evolve-ability, of an individual, collective or system to rapidly adapt to, and evolve *through*, crises. While logics of pre-emption employ the 'sciences of life' to better perform the sovereign function of 'making die', resilience employs this very same knowledge to potential-ize life processes so it can *really* live. Strategies of resilience thus engage with threats at the dangerous level of beating them at their own game: by entering a race to out-perform, out-adapt, and evolve quicker than threat-itself.

The Civil Contingencies Secretariat is not directly involved with the direction of an emergency response, but instead seeks to optimise the conditions necessary for a self-sufficient, emergent organizational evolution in the event of a crisis. As Bruce

Mann, the Head of the Civil Contingencies Secretariat puts it, “Our approach is to enable and to encourage.”⁴ A resilient telecommunication infrastructure is considered a ‘fundamental enabler’ for resilience. To gain a better appreciation of the relation of communications technologies to ‘resilience’ we shall turn our attentions briefly to the Revolution in Military Affairs (RMA).

The Need for Speed: A military genealogy

It has been said that war has long provided a grid of intelligibility for liberal governance (Foucault, 2003). To the extent that radical uncertainty is likewise said to characterize contemporary military applications (Dillon and Reid, 2009, Dillon and Reid, 2001), an avenue has opened for the transfer of military solutions to address this security problematic in civil applications. The Revolution in Military Affairs (RMA) in particular, has sought to confront the radical contingency of the battle environment by encouraging the development of emergent and adaptive military structures, and has thus been influential in informing emergency preparedness and response plans. To the extent that the RMA could be described as ‘revolutionary,’ the military strategy which it seeks to advance places an emphasis on rapid adaptability to environmental conditions, rather than fortitude, as the key merit in adjusting to this newly conceived battle-environment. To this end, military strategists have drawn heavily on the insights of complexity theory: the science behind self-organizing evolutionary systems (Cebrowski and Gartska, 1998, Moffat, 2003).

The transition to a more highly adaptive military structure was premised on a shift from the weapons platform to the information network, as the central

⁴ Bruce Mann, ‘Protecting the UK’s critical national infrastructure’, *Contingency Today*, http://www.contingencytoday.com/online_article/Protecting-the-UK_s-Critical-National-Infrastructure/416 accessed: 18 August 2008.

organizational principle for all levels of military organization (Cebrowski and Gartska, 1998). At the unit level, the information network became the source for new tactical approaches within a doctrine of network-centric warfare (cf. Alberts et al., 1999, Arquilla and Ronfeldt, 2001, Arquilla and Ronfeldt, 1997). The communications network is utilized to exacerbate communication between small bands of highly networked troops contributing to shared situational awareness amongst members of the unit. Shared situational awareness accelerates the completion of complex tasks and facilitates bottom-up organization, or ‘self-synchronization (Cebrowski and Gartska, 1998) of the unit permitting an emergent response to constantly evolving battle space.

According to the doctrine’s architects, the principal benefit to be gained from the transitional to network-centric style of warfare is to be found in the competitive advantage gained within the speed of command (Cebrowski and Gartska, 1998). The competitive advantage in speed, whereby threats can be responded to and opportunities capitalized on more quickly than the opponent, permits small bands of troops to overwhelm more numerous adversaries and decisively arrive at victory. The most important factor in generating speed of command is a highly robust communications infrastructure, which can be more or less addressed through advances in technology and systems design. The more problematic factor, relates to the human capacity to process information in order to come to a decision:

Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions. The joint force must be able to take advantage of superior information converted to superior knowledge to achieve “decision superiority” – better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. Decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and

experience, and the proper command and control mechanisms and tools are equally necessary. (Director for Strategic Plans and Policy, 2000)

Within this framework the capacity for soldiers to quickly process information and arrive at decisions is a guiding problematic for strategies seeking to instantiate and optimize processes of self-synchronization.

USAF Colonel John Boyd's OODA loop (Observe-Orient-Decide-Act) is commonly used as a model for the decision-making processes of a soldier within texts on self-synchronization.⁵ The OODA loop represents, in short, a cybernetic feedback loop in which environmental conditions are assessed, then used as the basis for a decision, which impacts the environment starting the whole processes again, ad-infinitum. Speed of command is accelerated by tightening the revolutions of the OODA loop of individual soldiers in a networked unit, which accelerates the unit's ability to make organizational adjustments within a rapidly evolving battle environment. Ideally, according to Vice-Admiral Cebrowski, self-synchronization would operate such that 'The "Observe-Orient-Decide-Act (OODA) Loop" appears to disappear, and the enemy is denied the operational pause. Regaining this time and combat power amplifies the effects of speed of command, accelerating the rate of change and leading to lock-out' (Cebrowski and Gartska, 1998). Note that the ideal time becomes that of the reflex: An immediate link between observation and action.

According to Boyd, efforts to close down the OODA loop must ultimately be directed at the problematic orientation phase, which "as the repository of our genetic heritage, cultural tradition, and previous experiences – is the most important part of the O-O-D-A loop since it shapes the way we observe, the way we decide, the way we

⁵ Colonel John Boyd's research has not been published, however his ideas have appeared in various literatures within the RMA including CEBROWSKI, A. K. & GARTSKA, J. J. 1998. Network-Centric Warfare: Its Origin and Future *US Naval Institute Proceedings*, 123, 1-24.

act” (Boyd, 1987).⁶ The Orientation phase links the intake of information, to the output of a decision and thus refers to the processes through which information is analyzed and synthesized in order to proceed to a decision. Strategies aimed at accelerating the OODA loop thus far operate not by seeking to order the cognitive processes themselves, but by optimizing the conditions of operability of these processes, in order to boost their speed and efficiency.

In particular, the prefrontal cortex has been targeted as a key component in accelerating the orientation phase of the OODA loop: the brain region where it is said emotion, anticipation and situational awareness culminate (Wesensten et al., 2005). Factors known to depress the functions of the prefrontal cortex, such as extreme temperature conditions, dehydration, high operational tempo and sleep deprivation, were found to slow subject’s ability to complete even simple psychomotor tasks (Wesensten et al., 2005). The complex cognitive tasks required by the soldier within the field, including the ability to maintain shared situational awareness, has thus made the constant monitor of the prefrontal cortex, through sensors and software applied to the soldier, a necessary component of network-centric operations (Wesensten et al., 2005). Alternative efforts have also been made to stimulate the functioning of prefrontal cortex through the provision of caffeinated chewing gum (Kamimori et al., 2004).

What military psychologists are ultimately interested in optimizing are the conditions in which complex decision-making processes reach maximal efficiency and speed. The strategies developed to achieve this task are directed at the prefrontal cortex insofar as it is perceived to be the location in which anticipation, as well as

⁶ BOYD, J. 1987. Organic Design for Command and Control. from <http://globalguerrillas.typepad.com/JohnBoyd/Organic%20Design%20for%20Command%20and%20Control.pdf> accessed August 19, 2010. Briefing accessed from <http://www.d-n-i.net/boyd/pdf/c&c.pdf>. May 19, 2009

other affective states, is seen to translate into higher levels of awareness of one's environment. The decision-making processes of the subject are black-boxed as a complexly constituted field in which decisions are emergent. Governance operates not by attempting to order these complex processes of cognition, but by optimizing their conditions of operability. Power, here, is not concerned with the specific coordination of actions, but in learning to modulate the anticipatory levels to induce reflexive, as opposed to reflective, decision-making (Massumi, 2005a: 33). As such, these strategies are related to 'the governance of affect' to which there is a growing literature (cf. Adey, 2008, Anderson, 2006, Massumi, 2005a, Massumi, 2005b).

Within the military psychological literature on the RMA, this has been strategized through efforts based on exciting the prefrontal cortex, which within this discourse, operates as a place of synthesis: between environment, and the multitude of strategies already embodied within the individual. The prefrontal cortex is targeted only insofar as it is considered to be related to the capacity of the individual to form relations: with technology, with the environment and with other bodies. Its capacity to form relations is profoundly influenced by the ways in which expectation is structured within the preconscious register of the subject. Varying the excitability of the prefrontal cortex gives control over the speed in which decisions are made insofar as it "assists in the germination of potentials for action, whose outcome could not be determined in advance" (Massumi, 2005a: 32-33).

Training-in resilience

Preparedness exercises are used extensively by the Civil Contingencies Secretariat as a technology for 'training-in' resilience. The UK Resilience website

promotes exercises as a necessary element of preparedness planning which can be used to test emergency plans and procedures, “develop staff competencies and give them practice in carrying out their roles in the plans”.⁷ Central government has organized a cross-governmental exercise programme to test the coordination of various tiers of emergency response--from central government and the Civil Contingencies Committee to regional and local response teams--to a wide range of challenges from natural disasters⁸ to viral pandemics⁹ to acts of terrorism.¹⁰ Exercises have been conducted in international joint operations with the G8, NATO, and the EU, as well as on a bilateral basis.¹¹ The Civil Contingencies Act Regulations mandates regular exercises for Category 1 responders to be organized by local or regional authorities.¹² The UK Resilience website provides guidance for businesses in the development of their own contingency plans through the Business Continuity Management (BCM) programme¹³ and promotes exercising these plans through

⁷ ‘Exercises’ *UK Resilience*, <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises.aspx> accessed: 20 August 2010.

⁸ ‘Exercise “Triton”’ *UK Resilience* (conducted June-July 2004,) <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/nationalcasestudies/triton.aspx> accessed: 20 August 2010.

⁹ ‘Exercise “Winter Willow”’ *UK Resilience* (conducted 30 January & 19-20 February 2007) http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/nationalcasestudies/winter_willow.aspx accessed: 20 August 2010

‘Exercise “Hawthorn”’ *UK Resilience* (conducted 5 April 2005) <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/nationalcasestudies.aspx> accessed: 20 August 2010

‘Exercise “Aurora”’ *UK Resilience* (conducted September 2005) <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/nationalcasestudies/aurora.aspx> accessed: 20 August 2010.

¹⁰ cf. ‘Exercise “Atlantic Blue”’ *UK Resilience* (conducted April 2005 in joint operation with the United States and Canada) <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/nationalcasestudies/atlanticblue.aspx> accessed: 20 August 2010.

¹¹ ‘National Exercises: Case Studies’ *UK Resilience* <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/nationalcasestudies.aspx> accessed: 20 August 2010.

¹² The Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 <http://www.cabinetoffice.gov.uk/media/132751/finalregs.pdf> (see 25, 31) accessed: 20 August 2010.

¹³ ‘Business Continuity’, *UK Resilience*, <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/businesscontinuity.aspx> accessed: 20 August 2010.

discussion-based, table-top and live exercises¹⁴ for the purpose of “helping participants develop confidence in their skills and providing experience of what it would be like to use the plan's procedures in a real event.”¹⁵

Recent scholarship has begun to examine preparedness exercises as a technology of risk-management. Davis traces the development of exercises during the Cold War as a technology for rendering a potential nuclear confrontation ‘imaginable, manageable and most of all capable of being acted upon, at least in part.’ (Davis, 2007: 3) Lakoff situates exercises, and the logic of ‘preparedness’, at the limit of insurance technologies, as a means for generating data on events which “cannot be mapped through actuarial knowledge and whose probability therefore cannot be calculated” (Lakoff, 2007: 253). Instead of relying on actuarial data, exercises render a future dystopian event through the imagination in relation to which plans can be tested and capabilities exercised which would be utilized in an ‘actual’ response. Cooper, suggests that the reliance on techniques of ‘speculative’ imagination resonate with wider trends towards contemporary trends towards speculative finance and a ‘speculative ontology of nature’ as methods for conceptualizing and operating in a world increasingly characterized as uncertain, or even ‘turbulent’ (Cooper, 2010).

As a speculative technology exercises do not aim to predict the future, but look to render *a* possible, dystopian future in relation to which faculties can be nurtured and capabilities exercised in preparation for a potential event which is itself unknowable. Insofar as they do not aspire to prophesy, exercises are not assessed in relation to predictive accuracy; true or false. Rather, they are assessed according to their ability to 1) generate feedback on existing plans 2) train-in required faculties of

¹⁴See especially the ‘Home Office guidance: The Exercise Planners Guide’ (1998) and ‘Home Office guidance: Why exercise your disaster response’ at ‘Exercises’ *UK Resilience*, <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises.aspx> accessed: 20 August 2010

¹⁵ ‘Exercises’ *UK Resilience*, <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises.aspx> accessed: 20 August 2010.

those associated with an emergency response and 3) to build personal and team confidence in the plans as well as personal and team abilities.

While considerable theorization has been placed on exercises as a risk-based technology for rendering the future actionable less attention has been paid to the processes of subjectivization inherent within preparedness exercises. Doing so would raise such questions as: what forms of subjectivity are valorised, how is agency and subjectivity conceptualized, and how do practices of governance seek to promote these forms? In asking these questions, it is also important to recognize that exercises are not simply sites of governance, but also technologies of governance: their particular design, as elucidated above and discussed in greater detail below, is intended to have governmental effects on the subject.

Davis accounts how verisimilitude is an important consideration in the design of an effective exercise insofar as it encourages participants to ‘suspend their disbelief’ (Davis, 2007). The suspension of disbelief is crucial for the tension manufactured within the design of the exercise to take-hold. As, resilience is associated with the confidence of having successfully performed similar functions within events of duress, preparedness exercises look to simulate events so that ‘learning’ can be achieved, and confidence fostered. Insofar as atmospheres of tension maximize ‘learning’, the manufacture of the affective environment of an exercise is a key consideration. A primary way in which this is achieved is through the manipulation of time. Exercises rarely proceed entirely in ‘real-time’. More often they are cut into segments in order to eliminate the dead-time between operations. Participant’s levels of excitability are further modulated by adjustments in the ‘battle-rhythm’ of the event: how quickly the events which need to be dealt with unfold.

‘Rising-tide’ exercises look to put into ‘play’ an emergent event; ‘sudden-impact’ events instead simulate more punctuated an event.

Preparedness exercises are geared towards habituation of decision-making under duress. While they undoubtedly are used to exercise plans, they also aim to foster the faculties of resourcefulness, flexibility and autonomy. As such, it resonates with wider trend in ‘advanced liberal governance’(Rose, 1999) of ‘responsibilising’ subjects to deal with their own risks (cf. Rose, 1996, Dean, 1999, O'Malley, 2004, O'Malley, 1996). Like insurance, exercises seek to fashion subjects capable of operating within a turbulent and uncertain world; a way of being-in-the-world which is not only confident in the ability to persevere through risk but which might even ‘embrace risk’ (Baker and Simon, 2002). Indeed regular exercises have the effect of inducing a disposition of permanent preparedness and, as such, can be regarded as useful in both “stimulating and disciplining the imagination” (Khan in Lakoff, 2007). Manipulation of the affective disposition of the subject for ‘training’ purposes creates autonomous subjects and ‘opens’ the subject more fully to technologies of governing through risk.

Conclusion: UK Resilience

“The Government's aim is to reduce the risk from emergencies so that people can go about their business freely and with confidence.” (UK Resilience Homepage)

"There is no liberalism without a culture of danger." (Foucault, 2008: 67)

This paper has taken preparedness exercises to be a technology of governance aiming to optimize subjectivities for accelerated emergency responses. At the governmental level, exercises look to fashion ‘resilient’ subjects capable of quickly compiling and processing a vast array of information in order to arrive at a decision.

To achieve this preparedness exercises look to simulate a high-tension environment in which decision-making under duress can be trained. In the process, the subject is ‘responsibilised’ by having learnt how to arrive at decisions confidently and quickly within uncertain and turbulent environments, allowing them to be autonomous and ‘free’. The objective of producing free and autonomous, ‘responsibilised’ subjects no doubt resonates with broader governmental trends associated with, what some authors have termed, ‘advanced liberal governance’ (Rose, 1999).

By focusing on the ways in which technologies of governance are directed at integrating the subject and ICT this paper sought to problematise conventional resilience discourses which treat communications technologies simply as a means for extending, or enhancing, the ‘natural processes’ of humans or collectivises to self-organize, permitting less governance and more ‘freedom’. An analysis of the regime of governance implicated in preparedness exercises draws attention to how the subject must likewise be managed and secured, in order for the potential of security technologies, which represent a condition for man’s ‘freedom’, to be fully realised. In the process, what is to be valued in, and about, the subject is framed in relation to the ability to integrate with and accelerate the processes of security technologies. To the extent that they fulfil this, what is valued in the subject are those faculties which optimize the technologies said to provide the conditions for their freedom.

Thus, while discourses of freedom and personal choice abound in resilience discourses this paper sought to study how correlative strategization, in what I have termed the ‘governance of affect’, reflects an intention of opening the subject more completely to this regime of risk-based forms of governance. It does so though attempts to modulate the anticipatory predisposition of the subject—a field of potentiality for action regarded as the key to accelerating decision-making. In doing

so governance of the subject shares a diagram of power associated with resilience more generally, in which power is directed towards optimizing the conditions of emergence for what are considered natural and highly efficient self-organizing (social, cognitive or technological) systems.

Overall these processes of subjectivization inherent within preparedness exercises allude to the prioritization placed on temporal, as opposed to spatial security, within resilience logics. Virilio uses the term 'chronopolitics' to refer to a trend in global politics away from spatial concerns such as territory to one concerned with the effects of temporal compression (Virilio, 1999, Virilio, 2005). While Virilio studied this trend in relation to processes of globalization (Virilio, 2005: 13) it is argued here that resilience should be thought of as a temporal security strategy which aims to minimize the duration of the catastrophic event. In distinction to spatial logics of security, aiming to prophylactically secure a space from threat through the construction of a barrier (ex. the fortress or bunker), resilience is a logic of security premised on eliminating a population's exposure to the emergency, not simply by mitigating vulnerability, but by minimizing the duration of the event itself.

Virilio points out the consequences of chronopolitics on processes of deliberation, negotiation and debate associated with contemporary democracy:

"The tyranny of real time is not very different from classical tyranny, because it tends to liquidate the reflective capacity of the citizen in favour of a reflex action. Democracy is about solidarity, not solitary experience, and humans need time to reflect before acting. Yet the real time and global present requires on the part of the telespectator a reflex response which is already of the order of manipulation." (Virilio, 1999: 87).

During an interview, Derrida was to describe the 'events' of September 11th as a 'major event'. A major event, Derrida states, is one which cannot be processed insofar as it exceeds our comprehension and appears outside our grids of intelligibility. The

major event then is *that which* I do not understand, but more precisely, the major event is *that* I don't understand—my incomprehension. (Derrida, 2003: 90). In articulating the ‘major event’ as such, Derrida echoes some contemporary understandings of trauma as an event whose meaning one is unable to allocate (cf. Caruth, 1995, Young, 1997). Edkins has argued that the time associated with trauma, or trauma time, is of deep political significance insofar as it disrupts the linear narratives of history underpinning sovereign power (Edkins, 2003). Resilience could thus be thought of as a strategy of keeping the event from becoming a ‘major event’ by habituating within the subject a regime of reflex-responses which are immediately instantiated, closing out the possibility of reflection, and soul-searching, on the ‘meaning’ (or lack thereof) of the event itself. This security regime, based on ‘de-eventalization’, operates by closing out reflection and thus the opportunity for political problematisation, or ‘critique’. Particular attention to the temporal dimension of resilience strategies, and their associated imperative for speed, are thus an important consideration for future studies.

References:

- ADEY, P. 2008. Airports, Mobility and the Calculative Architecture of Affective Control. *Geoforum*, 39, 438-451.
- ADEY, P. 2009. Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space*, 27, 274-295.
- ALBERTS, D. S., GARSTKA, J. J. & STEIN, F. 1999. *Network Centric Warfare*, Washington D.C., CCRP.
- ALLENBY, B. & FINK, J. 2005. Toward Inherently Secure and Resilient Societies. *Science*, 309.
- ANDERSON, B. 2006. Becoming and being hopeful: towards a theory of affect. *Environment and Planning D: Society and Space*, 24, 733-752.
- ARADAU, C., LOBO-GUERRERO, L. & MUNSTER, R. V. 2008. Security, Technologies of Risk, and the Political: Guest Editor's Introduction. *Security Dialogue*, 39, 147-154.
- ARQUILLA, J. & RONFELDT, D. (eds.) 1997. *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND.
- ARQUILLA, J. & RONFELDT, D. 2001. *Swarming and the Future of Conflict*, Santa Monica, CA, RAND.
- ARSENAULT, D. & SOOD, A. 2007. Resilience: A System Design Imperative. *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*. George Mason University.
- BAKER, T. & SIMON, J. (eds.) 2002. *Embracing Risk: The Changing Culture of Insurance and Responsibility*, Chicago: University of Chicago Press.
- BOYD, J. 1987. Organic Design for Command and Control. from <http://globalguerrillas.typepad.com/JohnBoyd/Organic%20Design%20for%20Command%20and%20Control.pdf> accessed August 19, 2010.
- CARUTH, C. (ed.) 1995. *Trauma: Explorations in Memory*, Baltimore: The John Hopkins University Press.
- CEBROWSKI, A. K. & GARTSKA, J. J. 1998. Network-Centric Warfare: Its Origin and Future *US Naval Institute Proceedings*, 123, 1-24.
- COOPER, M. 2006. Pre-empting Emergence: The Biological Turn in the War on Terror. *Theory, Culture and Society*, 23, 113-135.
- COOPER, M. 2010. Turbulent Worlds: Financial Markets and Environmental Crisis. *Theory, Culture & Society*, 27, 167-190.
- DAVIS, T. C. 2007. *Stages of Emergency : Cold War nuclear civil defense*, Durham, N.C., Duke University Press.
- DE GOEDE, M. & RANDALLS, S. 2009. Precaution, preemption: arts and technologies of the actionable future. *Environment and Planning D: Society and Space*, 27, 859-878.
- DEAN, M. 1999. *Governmentality : power and rule in modern society*, London, Sage.
- DERRIDA, J. 2003. Autoimmunity: Real and Symbolic Suicides. In: BORRADORI, G. (ed.) *Philosophy in a Time of Terror: Dialogues with Jürgen Habermas and Jacques Derrida*. Chicago: University of Chicago Press.
- DILLON, M. 2007. Governing Terror: The State of Emergency of Biopolitical Emergence. *International Political Sociology*, 1, 7-28.
- DILLON, M. & REID, J. 2001. Global Liberal Governance: Biopolitics, Security and War. *Millennium: Journal of International Studies*, 30, 41-66.

- DILLON, M. & REID, J. 2009. *The Liberal Way of War: Killing to Make Life Live*, Milton Park, Routledge.
- DIRECTOR FOR STRATEGIC PLANS AND POLICY, J., STRATEGIC DIVISION 2000. *Joint Vision 2020*. Washington: GPO.
- EDKINS, J. 2003. *Trauma and the Memory of Politics*, Cambridge, Cambridge University Press.
- ENVIRONMENT AGENCY 2005. *Working Together for a Better Flood Response: Exercise Triton 04 Overview Reports of Lessons Identified*.
- FOUCAULT, M. 2003. *Society Must Be Defended : lectures at the Collège de France, 1975-76*, London, Penguin.
- FOUCAULT, M. 2008. *The Birth of Biopolitics: lectures at the Collège de France, 1978-1979*, Basingstoke, Palgrave Macmillan.
- GORMAN, S. P. 2005. *Networks, Security and Complexity: The role of public policy in critical infrastructure protection*, Cheltenham, Edward Elgar Publishing Ltd.
- GOVERNMENT OFFICE FOR THE SOUTH EAST 2007. *Exercise Winter Willow 2: National and Regional Multi-level Joint Exercise, Post-exercise Report*.
- GRANT, M. 2010. *After the Bomb: Civil Defence and Nuclear War in Britain, 1945-68*, Houndmills, Basingstoke, Palgrave Macmillan.
- KAMIMORI, G. H., JOHNSON, D., BELENKY, G., MCLELLAN, T. & BELL, D. 2004. Caffeinated Gum Maintains Vigilance, Marksmanship, and PVT Performance During a 55-Hour Field Trial. *Proceedings of the 24th Annual Army Science Conference*.
- KEATING, J. P. 1982. The myth of panic. *Fire Journal*, 147, 56-61.
- LAKOFF, A. 2007. Preparing for the Next Emergency. *Public Culture*, 19, 247-271.
- LENTZOS, F. & ROSE, N. 2009. Governing insecurity: contingency planning, protection, resilience. *Economy and Society*, 38, 230-254.
- LOBO-GUERRERO, L. 2010. The International Political Sociology of Risk. *ISA Compendium Project*, International Studies Association.
- MANN, B. 2007. Protecting the UK's critical national infrastructure. *Contingency Today*.
- MASSUMI, B. 2005a. Fear (The Spectrum Said). *Positions*, 13, 31-48.
- MASSUMI, B. Year. The Future Birth of the Affective Fact. In: *Genealogies of Biopolitics Conference, 2005b* (accessed online 10 January 2009 <http://www.radicalempiricism.org/biotextes/textes/massumi.pdf>).
- MASSUMI, B. 2009. National Enterprise Emergency: Steps Towards an Ecology of Powers. *Theory, Culture & Society*, 26, 153-185.
- MOFFAT, J. 2003. Complexity Theory and Network-Centric Warfare.
- MULLER, B. J. 2008. Securing the Political Imagination: Popular Culture, the Security Dispositif and the Biometric State. *Security Dialogue*, 39.
- O'BRIEN, T. H. 1955. *Civil Defence*, London, Her Majesty's Stationery Office.
- O'MALLEY, P. 1996. Risk and responsibility. In: BARRY, A., OSBORNE, T. & ROSE, N. (eds.) *Foucault and Political Reason: Liberalism, neo-liberalism and rationalities of government*. London: USL Press Limited.
- O'MALLEY, P. 2004. *Risk, Uncertainty and Government*, London, The Glasshouse Press.
- QUARANTELLI, E. L. 1977. Panic Behavior: Some Empirical Observations. In: CONWAY, D. J. (ed.) *Human Response to Tall Buildings*. Stoudsburg: Dowden Hutchinson & Ross.

- QUARANTELLI, E. L. & DYNES, R. R. 1972. When disaster strikes (it isn't much like what you've heard and read about). *Psychology Today*, 5, 66-70.
- ROSE, N. 1996. The Death of the Social? Re-figuring the territory of government. *Economy and Society*, 25, 327-356.
- ROSE, N. 1999. *Powers of Freedom: reframing political thought*, Cambridge, Cambridge University Press.
- SIME, J. D. 1983. Affiliative Behaviour During Escape to Building Exits. *Journal of Environmental Psychology*, 3, 21-41.
- UK RESILIENCE 2007. Exercise Winter Willow: Lessons Identified. Department of Health (DH).
- VIRILIO, P. 1999. *Politics of the Very Worst*, New York, Semiotext(e).
- VIRILIO, P. 2005. *The Information Bomb*, London, Verso.
- WESENSTEN, N., BELENKY, G. & BALKIN, T. 2005. Cognitive Readiness in Network-Centric Operations. *Parameters*, 94-105.
- YOUNG, A. 1997. *The Harmony of Illusions: Inventing Post-Traumatic Stress Disorder*, Princeton, Princeton University Press.
- ZEBROWSKI, C. 2009. Governing the Network Society: A Biopolitical Critique of Resilience. *Political Perspectives*, 3, 1-38.