Risk and Surveillance After 9/11

By: Paul Simon
Student# 4872301
August 16th 2012

INTRODUCTION

The events which transpired on September 11, 2001 initiated a number of dramatic changes, some of which no doubt remain unrecognized or unknown. But one thing that has become obvious is the extent to which terrorism now occupies a critical position within political discourse, official policy-making, the popular imagination, academic analysis, and many other fields of social activity. And the fact that terrorism has come to occupy such a position reflects another, perhaps more ominous 'fact': the threat of terrorism now casts a rather haunting shadow over the political, economic, social, and cultural well-being of Western liberal democratic states. Hence, the threat of terrorism is treated as a *risk* by academics, senior government officials, the general public, and commentators.[1]

A host of problems emerge when the threat of terrorism is treated as a risk, not least of which pertains to the difficulty of precisely clarifying what kind of risk terrorism represents. For example, the threat of a terrorist attack is clearly a fundamentally different kind of risk than is, say, the risk of being struck by lightning. This is evident even without taking into account differences in terms of probability, for we need only recognize that terrorist attacks are carried out by human beings, are always planned and organized, are often based on strategic calculations, etc. It goes without saying that the same cannot be said of a lightning strike. Here the important point is that the difference between the risk of a lightning strike and the risk posed by the threat of a terrorist attack revolves around the fact that there are instantiations of

[1] For example, in *Catastrophe: Risk and Response* Richard Posner treats bioterrorism (or a terrorist attack which is carried out with the use of harmful biological agents, such as anthrax or sarin gas) as a catastrophic risk that has the potential to devastate large segments of a domestic or even international population. According to Posner, "[t]he danger of a cataclysmic bioterrorist attack seems so great that one may wonder why we are still here" (Posner 2004: 82). Indeed, "[b]ecause the biotech industry is expanding rapidly and the costs and skills required for gene splicing are falling, the danger of bioterrorism is rising. We may be safe today, but not tomorrow" (Posner 2004: 83).

risk which differ substantially in kind. This suggests that the problem of elucidating what kind of risk the threat of terrorism represents is closely connected to an even more difficult problem, namely, the problem of understanding what risk is. Thus, the problem of how to construe the risk posed by the threat of terrorism is intimately related to the problem of how to think of risk more generally.

The amount of recent scholarly work on risk is evidence in itself that there is no consensus as to how one ought to construe risk in a general sense. Three of the most influential sources of research on risk and its significance for our thinking about virtually everything associated with the hopelessly vague notion of 'modernity', are Ulrich Beck's *Risk Society* and the numerous texts that have drawn on the ideas introduced in Beck's work; Ian Hacking's *The Taming of Chance*; and a body of research that has come to be known as 'governmentality studies'. Each line of inquiry treats risk (in a general sense) quite differently. So, for example, generally speaking Beck thinks of risk as "a *systematic way of dealing with hazards and insecurities induced and introduced by modernization itself*. Risks, as opposed to older dangers, are consequences which relate to the threatening force of modernization and to its globalization of doubt [original emphasis]" (Beck 1992: 21). By characterizing risk as a 'systematic way of dealing with hazards and insecurities induced and introduced by modernization itself', Beck is attempting to capture two interconnected themes: on the one hand, risk is a way of thinking (risk thinking), a peculiar cultural artefact (a relatively coherent matrix constituted through the assemblage of discursive, ideational and practical elements) produced by modernity itself. On the other hand, *risks* are characterized as events to be treated in accordance with the perspective rendered possible by the aforementioned artifact.

Importantly, in every case risk is always a rather uniform or homogenous phenomenon generated by the movement of modernity. Furthermore, an especially unique characteristic of this more general phenomenon is its reflexive character.

In contrast to Beck, Hacking writes "of the taming of chance, that is, of the way in which chance or apparently irregular events have been brought under the control of natural or social law" (Hacking 1990: 10). In this particular context, Hacking views risk in connection with 'chance', where the latter came to be perceived, encountered, and grappled with as a peculiar metaphysical, cosmological, and quasi-scientific paradox of Western intellectual and cultural activity. In addition, Hacking also sets out to show how the history of the origin of chance may be interpreted, at least in part, as a history of Western intellectual and cultural development. According to this account chance (and by extension risk) is not simply a product of modernity but, rather, actually functions as a *condition* of modernity itself.

The third approach to risk tends to conceptualize risk as a "family of ways of thinking and acting, involving calculations about probable futures in the present followed by interventions into the present in order to control that potential future" (Rose 2001: 7). This is why Claudia Aradau and Rens van Munster are inclined to argue that "risk is multiform and heterogeneous, its rationality and logic are to be derived from an attentive analysis of configurations of practices" (Aradau and van Munster 2007: 98). The approach offered by governmentality studies is to be understood in stark contrast with Beck's analysis of risk. According to Aradau and van Munster, "Beck wrongly assumes that risks have the same features independent of the sphere in which they are articulated (e.g., environment, medicine, security, energy, the clinic). Risk is viewed as something given in the world and not as

something constructed" (Aradau and van Munster 2007: 101). More importantly, this also means that a "governmental analysis of risk is able to expose how the world and existing problematisations are made into risks, what effects this form of ordering entails upon populations. It is also able to understand changes in the modes of governing through risk depending on representations of the problem at hand and the subjects to be governed" (Aradau and van Munster 2007: 103).

Each of the aforementioned perspectives on risk has its own merits, and therefore each should be viewed as a suitable source of insight into the problem of how to understand the risk that the threat of terrorism represents. However, in the following discussion I intend to explore this problem by adopting a governmentality approach. The impetus behind doing so is based on the idea that the imperative introduced by the risk of a future terrorist attack is one which, interestingly enough, performs a governance function. This point is raised by Louise Amoore and Marieke De Goede, who argue that, "[f]rom the protection of borders to international financial flows, from airport security to daily financial transactions, risk assessment is emerging as the most important way in which terrorist danger is made measurable and manageable" (Amoore and De Goede 2005: 149). Indeed, after 9/11 there has been a number of policy responses designed to protect the United States – its resources, interests, institutions, and population – against any future harm resulting from another terrorist attack. And it should come as no surprise that one area within which this is most evident is in the field of intelligence and security.

Arguably at least some post-9/11 developments related to *domestic* security and intelligence can be explained on the basis of the fact that the threat of terrorism poses a

singularly unique and difficult problem, which is expressed by Paul Pillar when he creates a hypothetical scenario depicting a group of conspirators coming together in order to hatch some fiendish and deadly plot. The problem, according to Pillar, revolves around the following question: "How do we learn of the plot?" And the difficulties associated with acquiring a detailed knowledge of the plot are not, of course, the most severe. Pillar points out that "[t]he target for intelligence is not just proven terrorists; it is anyone who *might* commit terrorism in the future [original emphasis]" (Pillar 2004b: 115). In a different text, Pillar formulates this problem more precisely: "[d]etecting the perpetrators of the next terrorist attack against the United States will therefore have to go beyond link analysis and increasingly rely on other techniques for picking terrorists out of a crowd" (Pillar 2004a: 105).[2]

This problem is an absolutely crucial consideration to keep in mind when thinking about the relationship between terrorism, risk, and surveillance in the post-9/11 era. To be sure, it highlights the fact that domestic counter-terrorism operations must be fundamentally oriented by the need to ensure that law enforcement authorities and intelligence agencies are able to effectively *pre-empt* the materialization of future terrorist attacks. Hence, the *risk* of a future terrorist attack necessitates an intervention in the present in order to undermine the possibility of its future materialization.

A number of scholars have recently pointed out that since 9/11, intelligence agencies, law enforcement authorities, and private companies working with these (public) actors, have

[2] Reg Whitaker also touches on the unique imperative introduced by the threat of terrorism in *A Faustian Bargain? America and the Dream of Total Information Awareness?* According to Whitaker, "[t]he attorney general has released new investigative guidelines for the Justice Department reflecting its mission to 'neutralize terrorists before they are able to strike,' and to shift emphasis from criminal investigation to crime 'prevention' (perhaps 'pre-emption' might be more appropriate than the traditional 'crime prevention')". In addition, "the FBI is authorized to use 'commercial data mining services to detect and prevent terrorist attacks, independent of particular criminal investigations'" (Whitaker 2006: 152).

become increasingly interested in the possibility that data mining may represent a solution to the aforementioned problem of how to identify terrorists before they successfully carry out an attack (Rubinstein, Lee, and Schwartz 2008).[3] Perhaps one of the most controversial data mining projects proposed since 9/11 falls into the category of pattern-based predictive data mining. This project, referred to as 'Total Information Awareness' (later renamed 'Terrorist Information Awareness'), was to be operated under the direction of the Pentagon. According to Peter Gill, "TIA sought to bring together in 'ultra-large all-source information repositories' a number of existing CIT programmes – identifying links from message traffic and open source data, collaborative tools for humans and machines to 'think together', language processing for non-linguists, identification of predictive indicators of terrorist attacks, biometric identification technologies and exploiting 'nontraditional data sources to enable early detection and warning of a bioterrorist event'" (Gill 2004: 476).

If data mining is a form of surveillance practice that is deployed in accordance with the need to address a specific kind of risk – in this case, the risk posed by the threat of terrorism – to what extent can it be explained by drawing on previous work within governmentality studies? Or, to be more precise: is the practice of pattern-based data mining informed by the same logic as any of the other risk-based rationalities that have been elucidated by scholars who adopt an analytic of government in order to explain contemporary security practice? I contend that, quite simply, pattern-based predictive data mining is a form of surveillance

[3] This paper is principally concerned with the use of data-mining applications in post-9/11 counterterrorism measures implemented or otherwise pursued by governmental departments and agencies within the United States. One reason why such a focus will be adopted is simply due to the lack of substantial research and publicly available documents pertaining to efforts, programs, or initiatives aimed at utilizing data-mining applications for domestic counterterrorism surveillance operations within Canada by governmental departments and agencies.

practice which *does not* operate in accordance with the logic of insurance, precaution, or preparedness. Furthermore, rather than view this as evidence that an analytic of government is not a particularly effective approach to this problem, I believe there is good reason to suspect that a fourth risk-based rationality has come to the fore but has not yet been clearly elucidated.

This paper will consist of three sections. In the first section I will introduce and briefly explain several concepts, focusing specifically on governmentality, governance, and rationality. The principal focus of this discussion aims to highlight how these concepts are generally understood within the governmentality literature, but this cannot be adequately accomplished without providing some indication as to how Foucault deployed these concepts in his later lectures. Drawing on the research of scholars working in the field of governmentality studies, I will then map out three distinct though closely connected governmental rationalities. These are insurance, precaution, and preparedness. Common to all of these rationalities is the centrality of risk. That being said, each rationality construes risk differently. This means that each necessitates forms of practice designed in accordance with the logic of the risk in question, and therefore each risk-based rationality is underpinned by a form of knowledge which renders not only the specific conception of risk, but also the relevant practices, intelligible. In every case, risk necessitates an intervention in the present, and although the precise nature of this intervention may vary depending on the specific kind of risk which is being addressed, the affect in the present is one which entails a form of governance. Of particular importance, here, will be establishing the precise points at which each of these rationalities, despite the centrality of risk for each, nevertheless differ from one another.

In the second section I will turn to a close consideration of data mining, understood here as a particular form of surveillance practice. According to Oscar Gandy, "[d]ata mining is a process that has as its goal the transformation of raw data into information that can be utilized as strategic intelligence within the context of an organization's identifiable goals" (Gandy 2006: 364). Because data mining is widely used in various ways by a number of corporations, non-governmental organizations, and academic researchers, Christopher Slobogin introduces what he refers to as a typology of data mining. According to this typology, data mining "can either be target-driven, match-driven, or event-driven" (Slobogin 2008: 322). Of particular interest for the purposes of this paper is 'event-driven' data mining, as this approach to data mining is characterized mainly by its ability to predict future events through an analysis of identifiable data patterns. Event-driven data mining, "also called pattern-based surveillance, is data mining designed to discover the perpetrator of a past or future event; in contrast to both target-based and match-based data mining, this type of data mining does not start with an identified suspect" (Slobogin 2008: 323). Instead, pattern-based predictive data mining begins at the aggregate level of the population and proceeds to locate the individual within the aggregate, thereby providing law enforcement authorities with the ability to, as Pillar puts it, 'pick terrorists out of a crowd'.

In the third section I intend to demonstrate why the use of pattern-based predictive data mining for domestic counterterrorism surveillance cannot be adequately explained through recourse to the logic of insurance, precaution, or preparedness. This represents a crucial problem. As a technology of surveillance practice, pattern-based data mining is fundamentally bound-up with the prevention of a potential risk. Gandy highlights this

consideration when he points out that, "[a]t its core, data-mining is concerned with prediction. Data-mining efforts are directed towards the identification of behavior and status markers that serve as reliable indicators of a probable future" (Gandy 2006: 364). But if pattern-based data mining cannot be explained through recourse to the aforementioned rationalities, there is good reason to suppose that there is a fourth risk-based rationality that needs to be illuminated. Tentatively speaking, I contend that this fourth risk-based rationality is premised on the logic of risk *pre-emption*. I then suggest that a rationality of risk pre-emption must be understood in connection with a completely different conception of risk, one which has not been elucidated by scholars working within governmentality studies. Lastly, I offer some thoughts on what this may mean for our understanding of certain post-9/11 developments in the field of intelligence and security.

SECTION ONE

In the governmentality literature, 'governmentality' is generally understood as an *analytical perspective*. "As an analytical perspective, then, governmentality is far from a theory of power, authority, or even of governance. Rather, it asks particular questions of the phenomena that it seeks to understand, questions amenable to precise answers through empirical inquiry" (Rose, O'Malley, and Valverde 2006: 85). Some of these questions include, though are certainly not limited to: "Who governs what? According to what logics? With what techniques? Toward what ends?" (Rose, O'Malley, and Valverde 2006: 85). Because any particular regime or system of governance is always a complex arrangement of socially determined artifacts, the 'objects' that are taken as the focus of analysis within governmentality studies are configurations of discourse, knowledge, and practice which, together, constitute an 'art of government'.

In order to clarify the relationship between knowledge (of that which is to be governed, or the object of governance), and the practice of governing, Pat O'Malley focuses on how Foucault sought to infuse the concept of 'government' with connotations invoked by the term 'mentality'. According to O'Malley, "[c]entral to the Foucaultian idea of mentality is indeed analysis of the ways of *thinking* about government – how problems and people are thought about, what solutions to problems are dreamed up, what ends are imagined as ideal outcomes. It is in this aspect of government that inventiveness is made explicit, together with the 'made-up' nature of things" (O'Malley 2009: 4). Similarly, Colin Gordon maintains that "[a] rationality of government will thus mean a way or system of thinking about the nature of the practice of government (who can govern; what government is; what or who is governed), capable of

making some form of that activity thinkable and practicable both to its practitioners and to those upon whom it was practiced" (Gordon 1991: 3). Hence, the relationship between knowledge and practice is such that the object of governance is constituted through the dual operation of technologies of government and an ideational 'framework' within which both the object and the practice of governance are rendered intelligible in their mutual determinacy. An analytic of government therefore seeks to illuminate how governance is conducted by inquiring into the conditions whereby something can become and continue to function as an object of government.

Gordon points out that Foucault comes to understand "the term 'government' in both a wide and a narrow sense. He proposed a definition of the term 'government' in general as meaning 'the conduct of conduct': that is to say, a form of activity aiming to shape, guide or affect the conduct of some person or persons" (Gordon 1991: 2). 'Government', then, is not solely the purview or responsibility or activity of 'a' government; rather, government is a practice which is pursued as much by the individual or any other actor (such as an institution or organization) as it is by the state: an individual may 'govern' themselves through the adoption or affirmation of certain guidelines for conduct. Graham Burchell emphasizes this point when, quoting Foucault, he writes: "Government, Foucault suggests, is a 'contact point' where techniques of domination - or power - and *techniques of the self* 'interact', where 'technologies of domination of individuals over one another have recourse to processes by which the individual acts upon himself and, conversely, . . . where techniques of the self are integrated into structures of coercion'" (Burchell 1993: 268).

Scholars interested in governmentality have identified three distinct modes by which risk has been theorized. These are insurance, precaution, and preparedness. In each case, the basic temporal relationship between present and future is retained, though the relation between the two differs depending on how risk is construed.

In a text which is generally regarded as an insightful and absolutely fundamental analysis of insurance, François Ewald explains how, at its core, insurance developed around the emergence of a very specific and unique conception of risk. Accordingly, "[r]isk in the meaning of insurance has three great characteristics: it is calculable, it is collective, and it is a capital" (Ewald 1991: 201). When considering the first characteristic of insurance risk, Ewald maintains that "[f]or an event to be a risk, it must be possible to evaluate its probability" (Ewald 1991: 201-202). The probability of a risk is ascertained through statistical analysis, which is capable of establishing "a regularity of certain events", in conjunction with "the calculus of probabilities applied to that statistic, which yields an evaluation of the chances of that class of event actually occurring" (Ewald 1991: 202). The consequence of viewing risk in such a way is that the consistent occurrence of certain probabilities acquires an objective character with its own regularity and, thus, lends itself to prediction.

The second crucial characteristic of insurance risk is that it is collective. "Whereas an accident, as damage, misfortune and suffering, is always individual, striking at one and not another, a risk of accident affects a population." This is why Ewald claims that "[s]trictly speaking there is no such thing as an individual risk; otherwise insurance would be no more than a wager. Risk only becomes something calculable when it is spread over a population" (Ewald 1991: 202-203). Perhaps the most important consideration which follows from the way

in which insurance treats risk is that, according to Ewald, "risk is first of all a characteristic of the population it concerns" (Ewald 1991: 203). [4] Thus, insurance construes risk not as something which can strike at the population from outside of it, but as an inherent and 'natural' property or characteristic of the population itself. In this way, the general form of 'risk' is such that risk is treated as an inevitability.

The final characteristic of insurance risk is based on the idea that "[w]hat is insured is not the injury that is actually lived, suffered and resented by the person it happens to, but a capital against whose loss the insurer offers a guarantee" (Ewald 1991: 204). That is to say, "[o]ne and the same event acquires a dual status: on the one hand, a happening with the uniqueness of the irreparable; on the other, an indemnified risk" (Ewald 1991: 204). Although this final characteristic of insurance risk is interesting insofar as it identifies a crucial compromise that insurance facilitates and, perhaps, necessitates, the most important point to keep in mind is that the risk threatens to inflict an injury or some other form of damage for which there is an acceptable and expected amount of financial compensation.

As I have already mentioned, there are several distinct modes by which risk has been theorized in the governmentality literature. Indeed, O'Malley enjoins his reader to recognize that "those writing in the governmentality literature have stressed that if we look beyond the blanket characterisation of risk as government in terms of probabilities, it is clear that we have been living through a period in which key institutionalisations of risk have *changed* in key ways"

[4] Quoting Ewald, Andrew Lakoff clarifies the specific way by which insurance treats risk as an inherent and 'natural' property or attribute of the population: "[t]he events that insurance typically takes up are dangers of relatively limited scope and statistically regular occurrence: illness, injury, accident, and fire. When taken individually, such events may appear as contingent misfortunes, but when their occurrence is plotted over a population, they show a normal rate of incidence. Knowledge of this rate, gained through carefully plotted actuarial tables, makes it possible to rationally distribute risk" (Lakoff 2007: 250).

(O'Malley 2009: 14). One of the ways in which specific institutionalizations of risk have changed has been discussed by Ewald and others when considering precautionary approaches to risk, where such approaches are to be differentiated from an insurance-based rationality.

In *The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution*, Ewald argues that "[t]he nineteenth and twentieth centuries were obsessed with the problem of accidents (work-related or automotive); we are now rediscovering the existence of disaster, but with the difference that disasters are no longer, as before, attributed to God and Providence, but to human agency. It is in this deeply disrupted context that the precautionary principle now appears" (Ewald 2002: 283). The precautionary principle emerged during the 1980's within the context of legal regimes – whether international, European community, or municipal – that were principally concerned with issues relating to environmental degradation, transnational health pandemics, and the liability of products manufacturers. When considering specifically those instances wherein the precautionary principle was invoked within a legal framework designed to address the issue of environmental degradation, Ewald claims that "the precautionary principle does not target all risk situations but only those marked by two principal features: a context of scientific uncertainty on the one hand and the possibility of serious and irreversible damage on the other" (Ewald 2002: 283-284). These two characteristics mark an altogether different conception of risk than the one which underpinned insurance.

Ewald raises two important considerations when clarifying what he means by 'context of scientific uncertainty'. First, he argues that "[t]he precautionary hypothesis focuses on the uncertainty of the relationship of causality between an action and its effects" (Ewald 2002: 286). In contrast to insurance, precautionary thinking is premised on the idea that there is a

loose causal relationship between a given action in the present, and some future possibility caused by that action. Importantly, though, the precise nature of this causal relationship is always ambiguous or ill-defined, i.e. it is uncertain. Indeed, "[t]he notion of precaution concerns a situation in which only a relationship of possibility, eventuality, plausibility, or probability between a cause and its effect can be envisaged" (Ewald 2002: 286).

On the other hand, though, uncertainty characterizes not only the precise nature of the relationship between an action in the present and some future event, but also the specificity of the future event. Hence, "[t]he precautionary hypothesis puts us in the presence of a risk that is neither measurable nor assessable – that is, essentially a non-risk" (Ewald 2002: 286).[5] This is why precautionary thinking stipulates that one must envision the 'worst case scenario', even if scientific uncertainty entails that the hypothetical 'worst case scenario' may never even happen. And because scientific uncertainty precludes the possibility of acquiring an explicit knowledge of the impending risk, precautionary thinking does not permit the objectification of risk, as one would find in insurance.

[5] Those familiar with Ewald's work will note that this is a somewhat contentious claim, as Ewald clearly maintains that "[p]recautionary logic does not cover risk (which is covered by prevention); it applies to what is uncertain – that is, to what one can apprehend without being able to assess" (Ewald 2002: 286). When considering this claim it certainly seems as though precautionary logic is not informed by a specific conception of risk. However, while the reader might be inclined to suggest that this represents a problem for my treatment of Ewald's text, it is also clear that Ewald *does* move in the direction of construing certain instances of uncertainty as instances of risk. During his discussion of Beck's 'risk society' thesis, Ewald suggests that "[t]hrough the notion of precaution, the experience of risk takes on three additional dimensions that build on the descriptions provided in *Risk Society*." Here Ewald is focusing on Beck's argument that "[r]isk is not only a danger, it is a social relationship between those who have technological power and those who benefit or perhaps suffer from it." This leads Ewald to conclude that "[w]ith precaution, we are witnessing a remarkable change in this schema. The problem is no longer so much to multiply the responsibility for risk and to organize the solvency of those who are liable through insurance, but rather to prevent certain risks from being taken. Not only is prevention taking precedence over compensation, we are also trying to anticipate and prevent risks whose existence has not been proven" (Ewald 2002: 296).

The ‘worst case scenario’ introduces another important consideration into precautionary thinking. In particular, it entails a conception of risk whereby risk is always envisioned as that which has the potential to cause ‘serious and irreversible damage’ for which there can be no compensation. “In fact, the precautionary principle does not focus so much on an individual injury, such as may be caused by an accident, as on collective ‘catastrophic’ injury” (Ewald 2002: 284). Furthermore, and perhaps most importantly, precautionary thinking posits the risk as an unfathomable and catastrophic event which is certainly *not* inevitable; it is merely a probability which is not amenable to statistical calculation.

An ultimately unpredictable catastrophe which has the potential to cause ‘serious and irreversible damage’ introduces a specific logic into our thinking of risk, and thereby also our conduct. The precautionary principle requires that any action is undertaken in accordance with a decision whereby the individual acts ‘as if’ their action could cause or otherwise engender a particularly undesirable consequence. In contrast to insurance, the ‘risk’ of precautionary thinking is construed as an unknowable though hypothetically possible future event which is caused by an action in the present. Hence, action which is likely to ‘cause’ such a consequence is identified as ‘risk-taking’, whereas action which is performed in order to avoid the unfortunate outcome is precautionary. Thus, because the risk of precautionary thinking is not inevitable, by modifying one’s behaviour *in the present* it is possible to mitigate or altogether eliminate the possible future risk from materializing as a catastrophic event.

In *Governing Through Risk: Taking Precautions, (un)knowing the Future*, Aradau and van Munster “argue that precautionary risk has emerged in the dispositif of risk to govern terrorism, where other technologies have proven fallible or insufficient. Precautionary risk has

modified or supplemented other technologies of risk management and has reconfigured them at the horizon of the double infinity of terrorism" (Aradau and van Munster 2007: 24). In particular, the authors argue that it is possible to discern the influence of precautionary risk in the post-9/11 security environment when one considers the ever increasing deployment of pervasive and largely hidden forms of surveillance. This is primarily because "[p]recautionary risk management implies the surveillance of all the population, of all flights for example, independent of existing intelligence. Hence more and more technologies of surveillance are indiscriminately targeted at the whole population: stop and search policies in the UK, biometric identifiers or the introduction of identity cards" (Aradau and van Munster 2007: 27). Indeed, according to Aradau and van Munster, this is a logical and necessary consequence of the logic of precautionary thinking, as "[t]he rationality of catastrophic risk translates into policies that *actively* seek to prevent situations from becoming catastrophic at some indefinite point in the future" (Aradau and van Munster 2007: 29).

But according to Andrew Lakoff, a number of measures which were introduced by policymakers in order to effectively address the risk of some catastrophic event cannot be adequately explained by through recourse to an analytical framework which privileges precautionary thinking. In *Preparing for the Next Emergency*, Lakoff argues that the prevalence of various forms of emergency preparedness, emergency planning, early warning and detection systems, worst case scenarios and disaster simulations, resource allocation for materials and supplies that could be required 'just in case' the catastrophe does occur, certain forms of expert training, and special provisions within the mandates and authorities provided to 'first

responders', are all taken to be indicative of an altogether different risk-based governmental rationality. Lakoff refers to this (third) risk-based rationality as 'preparedness'.

> Like precaution, preparedness is applicable to events whose regular occurrence cannot be mapped through actuarial knowledge and whose probability therefore cannot be calculated. In contrast to precaution, however, preparedness does not prescribe avoidance; rather, it enacts a vision of the dystopian future in order to develop a set of operational criteria for response. Preparedness does not seek to prevent the occurrence of a disastrous event but rather assumes that the event will happen. Instead of constraining action in the face of uncertainty, preparedness turns potentially catastrophic threats into vulnerabilities to be mitigated (Lakoff 2007: 253).[6]

One way to appreciate the differences between preparedness and the other two risk-based rationalities outlined in the preceding discussion, is by focusing specifically on the way in which preparedness conceptualizes risk: in the case of preparedness, risk is always catastrophic (in the sense that it will cause irreparable and irremediable harm). Similarly, it is always irregular and unknowable. This is where preparedness differs fundamentally from *insurance*. But the point at

[6] To claim that 'preparedness does not seek to prevent the occurrence of a disastrous event but rather assumes that the event will happen' is very different from saying that 'preparedness assumes that the event *might* happen'. This difference is subtle and deserves close attention. Arguably, Lakoff maintains that preparedness assumes that the event will happen because the examples of preparedness thinking he uses in order to build his analysis are all catastrophic disastrous events which acquire the character of the inevitable through the way that they are represented discursively, theoretically, and practically. Lakoff argues that preparedness thinking actually emerged in the United States during the early years of the Cold War, and that this form of thinking was necessitated by the threat of an impending nuclear war with the Soviet Union. Hence, nuclear strategy, civil defense planning, as well as the creation of economic and political structures imperative for the continuation of life after a nuclear attack, were all informed by the logic of preparedness thinking. Lakoff argues that the end of the Cold War did not spell the end of preparedness. Rather, the techniques and systems put in place during the Cold War were reconfigured in order to mitigate other catastrophic events, such as natural disasters like earthquakes and hurricanes. Lakoff shows why, whether one is considering nuclear war or natural disasters, it is imperative that the possibility is always construed as an inevitability; that it is not a question of if another earthquake will happen, but when. Importantly, Lakoff contends that terrorism, too, is often represented by official policymakers and practitioners as though it is inevitable. Indeed, it is largely for this reason that the logic of preparedness thinking, together with the technologies, practices, and discourse which have traditionally formed a preparedness framework, can inform counterterrorism policy. However, although Lakoff claims that preparedness assumes an event will happen, this assertion does not leave room for the possibility that various forms of counterterrorism practice accord with a line of thinking which posits the possible, and not simply the highly probable, as a legitimate basis for action. This is an important insofar as it suggests that preparedness is actually a heterogeneous rationality: i.e., that in some areas it allows posits the highly probable, while in other areas it only requires the hypothetical and merely possible. The significance of this distinction lies in its implications for our understanding of the politics of preparedness in the post-9/11 age.

which preparedness differs most radically from *precaution* is where the risk that preparedness anticipates is construed in such a way that it is *not* loosely caused by any set of actions that could be modified in order to prevent the risk from materializing. In this sense, preparedness treats the impending risk as inevitable *and* unavoidable.

By positing this alternative conception of risk, preparedness necessitates a fundamentally different kind of conduct.

> Since the probability and severity of such events cannot be calculated, the only way to avert catastrophes is to have plans to address them already in place and to have exercised for their eventuality — in other words, to maintain an ongoing capability to respond appropriately. Although the probability and severity of a given event are not known, one must behave as if the worst-case scenario were going to occur — that it is not a question of if, but when. The point is to reduce current vulnerabilities and put in place response measures that will keep a disastrous event from veering into unmitigated catastrophe (Lakoff 2007: 253-254).

In a certain sense preparedness reflects a form of action which is reactive in terms of its logic and the implications that this has for practice. That is to say, even though preparedness thinking requires government authorities or individuals to undertake certain actions in the present in order to mitigate the anticipated consequences of a future catastrophe, preparedness is reactive in the sense that the present action always takes the form of a response. In contrast, as we have seen, precautionary thinking identifies activity in the present as a form of actively averting the potential catastrophe through the modification of behavior in the present which is likely to 'cause' that future event.

According to Lakoff, a number of developments in post-9/11 domestic security practice demonstrate that preparedness thinking has become a predominant risk-based governmental

rationality. In particular, Lakoff contends that a number of policies introduced by the Department of Homeland Security (DHS) represent the clearest example of this transformation.

> The demand for a coherent domestic security system that would consolidate multiple governmental prevention and response systems crystallized, after the attacks of September 11 and the anthrax letters, in the formation of the Department of Homeland Security. The new department brought together security functions from a number of areas of government: civil defense, disaster response, border security, intelligence, and transportation security (Lakoff 2007: 266-267).

Although the DHS is responsible for ensuring preparedness against a whole range of potential threats to, for example, critical infrastructure, since 9/11 the risk of a catastrophic terrorist attack has oriented much of the work that the DHS performs. Some of these include the execution of emergency scenarios such as 'Dark Winter' in 2001, 'Silent Vector' in 2002, 'Scarlet Cloud' in 2003, 'TOPOFF 3' in 2005, and 'Atlantic Storm' (also in 2005). These simulations were all geared towards exposing vulnerabilities in national 'systems' – whether food distribution systems, communications, health, public utilities, and transportation system – that could be disrupted by a 'conventional', biological, or chemical attack launched by terrorists within the United States (Lakoff 2007: 265-266).

On the basis of what has been discussed so far, it is clear that Aradau and van Munster, as well as Lakoff, argue that the risk-based rationalities they outline provide some insight into understanding post-9/11 domestic security practices in the United States. That being said, neither Aradau and van Munster, nor Lakoff, are attempting to provide an account of post-9/11 security practices (designed to address the threat of terrorism) which are exclusive and all-encompassing in terms of their ability to explain *all* such practices through recourse to a *single* governmental rationality. That is, arguably these authors would accept the possibility that

certain elements of security practice are best explained through recourse to a rationality of preparedness, and others are best explained by taking into account a rationality of precaution. However, I contend that contemporary surveillance technologies deployed by intelligence agencies, law enforcement authorities, and security organizations cannot be adequately explained on the basis of insurance, precaution, or preparedness. Instead, I suggest that these practices are best understood in terms of a logic of risk *pre-emption*. Thus, I not only contend that there is a fourth risk-based rationality which has yet to be elucidated; the position I intend to outline also diverges from Aradau and Van Munster, who argue that post-9/11 surveillance practice operates in accordance with the logic of precaution.

Admittedly this might, at first glance, seem like a rather contentious position. However, recent scholarly work in the field of surveillance studies indicates that pattern-based data mining is a form of surveillance practice which has attracted a great deal of attention from governmental departments and agencies responsible for preventing the occurrence of a potential terrorist attack. Posner writes that, "[i]n the wake of the 9/11 attacks, law enforcement authorities have, for example in the MATRIX project, pooled more and more of the information about individuals that is contained in different databases." And "[i]n the not very distant future, advances in digitization may enable the inexpensive creation of a comprehensive, continuously updated, readily accessible dossier on every human being on earth…" (Posner 2004: 86). Although this may seem somewhat alarmist, a number of scholars working in the field of surveillance studies point to concrete policy initiatives and government

projects which aim at 'total information awareness'.[7] And this, in turn, represents a form of surveillance practice which is fundamentally preemptive insofar as it is used to detect a potential threat which is likely to materialize in the future, thereby providing officials with reason to intervene in the present in order to ensure that the potential threat does not have the ability to materialize into an actual threat. Importantly, though, in this case any potential threat is not one which is in some way 'caused' by an action or set of actions undertaken in the present by an individual or group of individuals who are willing to modify their behavior in order to avert the catastrophe. It is for this reason that one cannot maintain, with Aradau and van Munster, that contemporary domestic surveillance measures deployed as part of a broader 'war on terror' are informed by a precautionary logic.

In the next section I intend to provide the reader with a brief history of data mining. I will then explicate some of the central concepts, principles, and techniques which inform contemporary practice. And lastly, I will discuss how, why, and in what ways, data mining has been deployed in the post-9/11 era as a means for addressing the risk posed by the threat of terrorism.

[7] Incidentally, 'Total Information Awareness', later called 'Terrorism Information Awareness', was the name of a program which, though cancelled by the United States Congress, was funded by the Department of Defense and, according to some scholars, continues to live on in a number of incarnations (Gill 2004; Solove 2008).

SECTION TWO

Since 9/11 a number of scholars and commentators continue to point out that various departments and agencies of the United States government have shown great interest in the potential of data mining technologies and applications (DeRosa 2004; Thuraisingham 2004; Last 2005). Indeed, there are a number of cases where the government has sought to develop, enhance, or otherwise introduce a powerful data mining capability as part of a much broader domestic security and counterterrorism effort. This is largely due to the belief (whether mistaken or not) that data mining applications are a highly effective means with which to identify individuals who are planning to carry out a terrorist attack (Elovici 2005; Seifert 2007; Cate 2008).[8] For this reason, data mining has come to be viewed as a crucial component of a comprehensive domestic surveillance regime.[9]

[8] Perhaps it should come as no surprise that the general rationale underpinning the 'promise' of data mining applications for the purpose of predicting potential terrorist attacks has come under intense scrutiny by academics, civil libertarians, columnists, and industry experts. Aside from a number of legitimate ethical concerns, most of which are closely related to the potential for abuse of personal information and violations of individual privacy, some critics have raised other, 'technical' concerns pertaining to the utility of data mining as an effective tool in the 'war on terror'. In *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, Jeff Jonas and Jim Harper argue that what they refer to as 'predictive' data mining, or pattern-based analysis, is of very limited use as a counterterrorist measure designed to "ferret out terrorists before they strike" (Jonas and Harper 2006: 6). Similarly, Seifert also points out that "[a]lthough data mining can help reveal patterns and relationships, it does not tell the user the value or significance of these patterns" (Seifert 2007: 3). For Seifert, then, the hype surrounding pattern-based data mining applications may be overblown.

[9] See, for example, an article entitled *The Surveillance Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society*. In this piece, Jay Stanley lists at least six examples of recent government data mining projects, intended to enhance domestic surveillance capabilities, which were introduced after 9/11. Also of interest is a 2007 CRS Report for Congress, entitled *Data Mining and Homeland Security: An Overview*, by Jeffrey Seifert, as well as a report released in 2006 by the Office of the Inspector General at the U.S. Department of Homeland Security. The latter, entitled *Survey of DHS Data Mining Activities*, states that: "[w]e identified 12 systems and capabilities that DHS personnel use to perform data mining activities to support DHS' mission of counterterrorism. Nine systems are operational and three systems are under development. While these data mining activities may perform various processes, we categorized and arranged our descriptions in a way that describes selected data mining processes and tools ranging from basic to advanced analytical tasks. The categories include expert systems, association processes, threat and risk assessment tools, collaboration and visualization processes, and advanced analytics" (DHS 2006: 4).

Generally speaking, scholars and industry experts tend to regard data mining as an emerging field which has its origins in conventional statistical analysis, advances in Artificial Intelligence (AI), and machine learning. In *Principles of Data Mining*, Hand et al. claim that "[d]ata mining is often set in the broader context of *knowledge discovery in databases,* or KDD. This term originated in the artificial intelligence (AI) research field. The KDD process involves several stages: selecting the target data, preprocessing the data, transforming them if necessary, performing data mining to extract patterns and relationships, and then interpreting and assessing the discovered structures" (Hand et al. 2001: 6-7). The impetus behind research into KDD was based on the possibility of extracting useful 'knowledge' from the rapidly increasing quantity of data that was being acquired, generated, and collected in a number of sectors throughout society. In this case, the knowledge in question could be used for everything from identifying consumer preference, fraud detection, or detecting wasteful business expenditures (Fayyad 1996: 38). Moreover, because data mining is used to 'make sense' of the data, it is often considered to be the most crucial step in this more general process. This is one reason why data mining in particular – that is to say, the systems and algorithms used to 'mine' data – has developed exponentially since the early days of KDD.

Although there may be general agreement about the origin of data mining, as Mary DeRosa rightfully points out in *Data Mining and Data Analysis for Counterterrorism*, "[o]ne of the first problems with 'data mining' is that there are varying understandings of what the term means" (DeRosa 2004: V). For example, Hand et al. construe data mining as "the analysis of (often large) observational data sets to find unsuspected relationships and to summarize the data in novel ways that are both understandable and useful to the data owner" (Hand et al.

2001: 6). As is evident, the authors do not mention specific data mining techniques, nor do they refer to any particular applications. Hence, it is difficult to establish why, based on the definition of data mining they provide, there is any meaningful difference between data mining and routine statistical analysis. In contrast, Fred Cate provides a clear and relatively comprehensive definition of data mining while mapping several of the principal techniques that are currently employed. According to Cate,

> 'Data mining' is defined in many different ways but is perhaps best understood as encompassing a wide spectrum of data-based activities ranging from 'subject-based' searches for information on specified individuals to 'pattern-based' searches for unusual or predetermined patterns of activities or relationships. Between these two ends are 'relational' searches, which start with an individual but then reach out to determine who communicates or otherwise interacts with whom, and 'data matching,' which involves combining two or more sets of data looking for matches or discrepancies (Cate 2008: 438).

While this is certainly a more comprehensive definition, it does not take into account the fact that the patterns, activities, or relationships which may be discovered through pattern-based data mining are not always 'predetermined'. In many cases, such patterns are 'discovered' in the sense of 'finding something new'; an original set of meaningful relationships which were previously unknown. This is what DeRosa is getting at when she says that "'[d]ata mining' actually has a relatively narrow meaning: it is a process that uses algorithms to discover predictive patterns in data sets" (DeRosa 2004: V).[10] This definition retains the idea that the

[10] DeRosa then proceeds to draw a distinction which, though interesting and to a certain extent warranted, other authors do not articulate. The distinction in question is between data mining and 'automated data analysis.' The precise nature of the difference between the two revolves around the fact that data mining is a technique used to discover patterns within extremely large structured and unstructured data sets, whereas automated data analysis involves the application of patterns derived through data mining in order to "predict behavior, assess risk, determine associations, or do other types of analysis. The models used for automated data analysis can be based on patterns (from data mining or discovered by other methods) or subject based, which start with a specific known subject" (DeRosa 2004: V). This distinction, as well as the relationship between data mining and automated data analysis, is important and worth further consideration. Unfortunately, I will have to put this

patterns which are 'discovered' through data mining are 'predictive', though it does not stipulate that these patterns are predetermined. The scope of the definition may be narrow insofar as it specifies that data mining is a process used to discover predictive patterns, but it leaves open the question as to whether the patterns are predetermined. An even more focused definition of data mining, which is nevertheless flexible enough to account for recent developments in data mining practice, is adopted by Collier et al. when quoting a definition initially formulated by Michael Berry and Gordon Linoff. According to Collier et al., "'[d]ata mining is the exploration and analysis, by automatic or semiautomatic means, of large quantities of data in order to discover meaningful patterns and rules'" (Collier et al. 1998: 2). This paper will follow the lead of Collier et al. and adopt this definition, which is to be used as a guide during the following discussion.

In *Data Mining: An Overview From a Database Perspective*, Chen et al. provide the reader with some indication of the various kinds of databases that can be mined using different data mining techniques and systems. The authors claim that, "[i]n general, a data miner can be classified according to its mining of knowledge from the following different kinds of databases: relational databases, transaction databases, object-oriented databases, deductive databases, spatial databases, temporal databases, multimedia databases, heterogeneous databases, active databases, legacy databases, and the Internet-information base" (Chen et al. 1996: 868). The crucial point, here, is simply that "[d]ata mining can be performed on data represented in quantitative, textual, or multimedia forms", such as imagery and in real-time video or communications traffic on the internet (Seifert 2007: 1). For example, in *Real Time Video Data*

---

aside, for the time being, in order to proceed with our discussion of the various definitions of data mining. However, I do intend to return to a more thorough examination of automated data analysis.

Mining for Surveillance Video Streams, Oh et al. introduce a model and claim that "[t]he examples of knowledge and patterns that we can discover and detect from a surveillance video sequence are object identification, object movement pattern recognition, spatio-temporal relations of objects, modeling and detection of normal and abnormal (interesting) events, and event pattern recognition" (Oh et al. 2003: 576).

Three of the most common and proven data mining techniques are clustering, link analysis, and pattern-based data mining. According to Fayyad et al., clustering "is a common descriptive task where one seeks to identify a finite set of categories or clusters to describe the data" (Fayyad et al. 1996: 45). In this particular case, a researcher will employ clustering in order to "group a set of data (without a predefined class attribute), based on the conceptual clustering principle: *maximizing the intraclass similarity while minimizing the interclass similarity*." So, for example, "a set of commodity objects can be first clustered into a set of classes and then a set of rules can be derived based on such a classification. Such clustering may facilitate *taxonomy formation*, which means the organization of observations into a hierarchy of classes that group similar events together [original emphasis]" (Chen et al. 1996: 868). Hence, clustering allows a researcher to group data into either predetermined categories established on the basis of an already given set of rules, or to discover new rules with which to group or categorize data which does not conform to previously known rules but nevertheless shares a number of sufficiently relevant similarities.

Unlike clustering, link analysis is 'subject-based' (in the sense that it looks at information or data pertaining to individuals, and is therefore not utilized when analyzing object-oriented data about stock prices, weather patterns, etc.) and "uses aggregated public records or other

large collections of data to find links between a subject—a suspect, an address, or other piece of relevant information—and other people, places, or things" (DeRosa 2004: 6). Here the objective is not to 'sort' the data in order to identify relevant groupings that could help to develop a profile or map recurring relationships between objects, places, subjects, or events. Rather, link analysis reveals "additional clues for analysts and investigators to follow" by sifting through volumes of data that would simply overwhelm human investigators and would thereby go unnoticed. For this reason, "[l]ink analysis is a tool that is […] used for, among other things, background checks of applicants for sensitive jobs and as an investigatory tool in national security and law enforcement investigations" (DeRosa 2004: 6).[11]

Arguably both clustering and link analysis may be considered data mining techniques which 'discover' or otherwise reveal 'patterns' in the databases they are used to mine. Indeed, arguably *any* data mining technique reveals meaningful patterns which are then used for a variety of purposes. A piece of data can only be meaningful or acquire any significance if it is located within a more general 'pattern', or a set of relationships between it and other items of data. On its own, a single item of data is virtually meaningless. Since all data mining techniques are ultimately used for revealing patterns, Fayyad et al. draw a distinction between *descriptive* patterns, such as those discovered through clustering or link analysis, and *predictive* patterns (Fayyad et al. 1996: 44). By doing so they are able to retain the idea that all data mining is, to a certain extent, concerned with identifying patterns, though they are able to differentiate between specific data mining techniques on the basis of whether or not they are descriptive or

[11] According to DeRosa, "[a] hindsight analysis of the September 11 attacks provides an example of how simple, subject-based link analysis could be used effectively to assist investigations or analysis of terrorist plans. By using government watch list information, airline reservation records, and aggregated public record data, link analysis could have identified all 19 September 11 terrorists—for follow-up investigation—before September 11" (DeRosa 2004: 6).

prescriptive. And, generally speaking, when referring to pattern-based data mining most authors have in mind techniques used to identify predictive patterns rather than descriptive patterns.

According to Chen et al., pattern-based similarity searches are employed "in order to discover and predict the risk, causality, and trend associated with a specific pattern. Typical queries for this type of database include identifying companies with similar growth patterns, products with similar selling patterns, stocks with similar price movement, images with similar weather patterns…" (Chen et al. 1996: 869). In this particular case, the idea is basically as follows: if one identifies a pattern which recurs with sufficient constancy throughout a determinate span of time, one can therefore predict the recurrence of that pattern within parameters established through analysis of previous occurrences. Hence, pattern-based data mining is typically utilized when mining temporal databases with a specific time-series function, as prediction always involves a temporal dimension.

Since 9/11, a number of government departments and agencies in the United States have sought to develop and deploy data mining techniques and applications as part of a more comprehensive strategy aimed at securing the homeland. To be sure, data mining has become a critical component of domestic intelligence and counterterrorism efforts. "In fact", writes K. A. Taipale,

> development of these technologies is already mandated by law as the Homeland Security bill signed by President Bush on November 25, 2002 contains provisions that specifically make it the responsibility of the Undersecretary for Information Analysis and Infrastructure Protection at the Department of Homeland Security to 'establish and utilize . . . a secure communications and information technology infrastructure, including data mining and other advanced analytical tools, in

> order to access, receive, and analyze data and information in furtherance of the responsibilities under this section . . . .' (Taipale 2003: 4).[12]

As we discussed above, clustering is generally used in order to group data into classes "based on the conceptual clustering principle: *maximizing the intraclass similarity while minimizing the interclass similarity* [original emphasis]" (Chen et al. 1996: 868). In effect, clustering allows one to identify groups of people by creating 'clusters' established on the basis of similar behavioral, physical, cultural, and socio-economic characteristics.[13] Clearly clustering is a technique that can be used for class formation, where the class (or specific attributes of the class) in question was not previously known to investigators. However, this also means that clustering may be used for classificatory purposes. In this particular case, a subject profile is established on the basis of certain characteristics derived from previously known cases. Such profiles then serve as a kind of 'template' which provides investigators with a means of identifying potential suspects.

According to Nasrullah Memon and Abdul Rasool Qureshi, link analysis "is the first level by which networks of people, places, organizations, vehicles, bank accounts, telephone calls, email contacts, and other tangible entities can be discovered, linked, assembled, examined, detected, and analyzed" (Memon and Qureshi 2005: 399). Here the focus is on identifying or

[12] Here Taipale is quoting directly from the published findings of a report by the Congressional Joint Committee Inquiry into the Terrorist Attacks of September 11, 2001. In addition to the aforementioned claim quoted by Taipale, evidence of government interest in developing advanced data mining capabilities to be utilized for domestic security is evident in the following passage from the Joint Inquiry report. "Fortunately, recent efforts to move forward in empowering analysts to conduct *true* all-source analysis provide reasons for confidence that a workable solution is possible. As the SSCI's Technical Advisory Group (TAG) – a nonpartisan group principally composed of expert private sector technologists and managers with the highest possible security clearances – has forcefully recommended, we must move forward into the realm of comprehensive databasing and data-mining *now*, and the technology we need is either in existence already or well on its way to development [original emphasis]" (Joint Inquiry 2002: 56). The Joint Inquiry report then proceeds to discuss a number of data mining projects operational at the time of the inquiry (and before 9/11), programs managed by the Department of Defense, the Justice Department, and the Central Intelligence Agency (CIA).

[13] For an example of what such a profile could look like – i.e., what kind of information could potentially be included in a profile – see appendix A.

revealing networks rather than taxonomy formation. To be more precise, link analysis "is often used to answer such questions as *who knows whom and when and where* [have] *they been in contact?*" (Memon and Qureshi 2005: 399).[14]

Although each of the aforementioned data mining techniques may be employed at different stages of a single surveillance operation or investigation, the remainder of this discussion will focus on illustrating how pattern-based predictive data mining, understood here as a specific technique of data mining, is being utilized by law enforcement authorities, intelligence agencies, and government departments in the United States since 9/11.

The development of sophisticated pattern-based data mining algorithms for domestic surveillance programs is closely linked to a rather unique challenge that intelligence agencies and law enforcement authorities have been faced with since 9/11. Assuming that there could be a number of terrorist 'sleeper cells' or even just a single 'lone wolf' currently planning to carry out an attack on American soil, how does the government identify the members of the cell or the lone individual and prevent them from carrying out the attack? Several authors and government documents provide good reason to believe that pattern-based predictive data mining is increasingly viewed as a potential solution to this problem. Indeed, "[u]nlike subject-based queries, pattern-based searches do not require a link to a known suspicious subject" (DeRosa 2004: 8). Rather,

> [i]n its pattern-based variant, data mining searches select individuals for scrutiny by analyzing large data sets for suspicious data linkages and patterns. Because terrorists do not 'stand out,' intelligence and law enforcement agents want to do

[14] Figures 1 and 2 in appendix B illustrate how link analysis can be used to graphically represent networks of people, such as the al-Qaeda command structure or the 9/11 hijackers. Interestingly, link analysis can also help one to establish directionality, which provides some insight into the kind of relationship and, by extension, the kind of actors one is dealing with, i.e., their authority or 'status' vis-à-vis one another within the network.

> more than rely exclusively on investigations of known suspects. The new goal is to search 'based on the premise that the planning of terrorist activity creates a pattern or 'signature' that can be found in the ocean of transaction data created in the course of everyday life' (Rubinstein et al. 2008: 261).

Arguably this is one of the most powerful reasons as to why pattern-based data mining is so alluring to government departments and agencies responsible for preventing the occurrence of another terrorist attack. "Terrorists lurk among us, and ferreting them out can be quite difficult. Examining data for patterns will greatly assist in this endeavor, the argument goes, because certain identifiable characteristics and behaviors are likely to be associated with terrorist activity" (Solove 2008: 346). This basic point is also raised by Rubinstein et al., who argue that "[i]n pattern-based data mining […] the government investigator develops a model of assumptions about the activities and underlying characteristics of culpable individuals or the indicators of terrorist plans" (Rubinstein et al. 2008: 262).

As was mentioned above, "[p]attern-based queries take a predictive model or pattern of behavior and search for that pattern in data sets." The idea, then, is that "[i]f models can be perfected, pattern-based searches could provide clues to 'sleeper' cells made up of people who have never engaged in activity that would link them to known terrorists" (DeRosa 2004: VI). This is precisely why, as Cate points out,

> [a]fter the terrorist attacks of September 11, 2001, pattern-based data mining struck many observers as a promising tool for law enforcement and national security. If government officials could develop models of what criminal or terrorist behavior might look like and then search for those patterns across a sufficiently broad range of information, observers hoped it would be possible to detect criminals or terrorists, perhaps even before they executed their nefarious enterprises. In the Homeland Security Act of 2002, Congress required the new Department of Homeland Security ('DHS') to 'establish and utilize . . . data-mining and other advanced analytical tools' to 'access, receive, and analyze data to detect and identify threats of terrorism against the United States' (Cate 2008: 439).

It is therefore important to note that the promise of pattern-based data mining is in large part based on the possibility of discovering patterns which correspond to already known or established patterns of terrorist behavior. This represents one (perhaps problematic) general approach to the use of pattern-based data mining for domestic security. However, it is also the case that "[t]he government uses these data sets for a spectrum of data mining activities, ranging from inquiries on specific individuals and the people with whom they interact to broad searches for unusual or predetermined patterns of activities or relationships" (Cate 2008: 436). Hence, a second general use of pattern-based searches focuses on revealing 'abnormalities' that could provide reason for suspicion and further, more intensive surveillance. In this case, the suspicious pattern is represented as an 'outlier' that does not conform to the expected norm or any predetermined pattern; in this way it raises a flag for investigators.

Cate provides some indication of the extent to which pattern-based data mining has been utilized by government departments as part of surveillance and counterterrorism measures.

> A 2004 report by the then-General Accounting Office ('GAO') found that forty-two federal departments—including every cabinet-level agency that responded to the survey—engaged in, or were planning to engage in, 122 pattern-based data mining efforts involving personal information. Thirty-six of those involve accessing data from the private sector; forty-six involve sharing data among federal agencies. Fourteen data mining programs in the GAO report are concerned with '[a]nalyzing intelligence and detecting terrorist activities' and fifteen involve '[d]etecting criminal activities or patterns' (Cate 2008: 439).

Another example of pattern-based data mining counterterrorism initiatives pursued by the government is a program called "ADVISE (for Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement), which was designed 'to troll a vast sea of information, including audio and visual, and extract suspicious people, places and other elements based on their links and

behavioral patterns" (Slobogin 2008: 318). In addition, Seifert claims that the National Security Agency (NSA) "has reportedly been supporting the development of new technology and data management techniques by funding grants given by the Advanced Research Development Activity (ARDA). ARDA is an intelligence community (IC) organization whose mission is described as 'to sponsor high-risk, high-payoff research designed to leverage leading edge technology to solve some of the most critical problems facing the Intelligence Community (IC)'" (Seifert 2007: 26). One of several programs ARDA is currently operating is referred to as the 'Novel Intelligence from Massive Data' (NIMD) program. Although there is not much known about this program, its aim is to identify "actionable information not previously known" through the application of cutting edge data analysis techniques, where such techniques are particularly effective at extracting intelligence from data "that has characteristics that are especially challenging to common data analysis tools and methods" (Seifert 2007: 26).

But to utilize pattern-based data mining in order to identify and 'map' a 'signature' which might reveal the intentions of an individual planning to carry out a terrorist attack, law enforcement authorities and intelligence agencies must have access to an incredible amount of data. Several scholars discuss in detail cases which demonstrate that the government, often in partnership with private actors, has begun to develop capabilities which facilitate access to the rapidly increasing volume of personal data.

Arguably there are two intertwined dimensions of the impetus behind the development and use of massive data storage facilities. First, Cate points out that

> [t]he government faces new and intense pressure to collect and use personal data. Much of that pressure reflects the conviction that greater reliance on digital data will reduce costs and enhance convenience, speed, efficiency, and accountability. Perhaps the greatest source of that pressure, however, is the fear

> of terrorist attacks and the widely shared view, as the National Commission on Terrorist Attacks Upon the United States (commonly referred to as the 9-11 Commission) Vice Chairman Lee Hamilton testified before Congress in November 2005, that the inability of federal agencies to marshal and share information about suspected terrorists and their activities 'was the single greatest failure of our government in the lead-up to the 9/11 attacks' (Cate 2008: 436).

After 9/11 the government faced enormous political pressure due in large part to its perceived failure to prevent the 9/11 hijackers from carrying out the attacks. This line of argument generally places a great deal of emphasis on the fact that intelligence agencies and law enforcement authorities actually had enough information about the 9/11 hijackers which, if they had shared it with one another, would enable them to 'connect the dots' and effectively identify and apprehend the perpetrators prior to the attacks. Indeed, this alleged failure was examined in *The 9/11 Commission Report*, which recommended that "[a] 'smart' government would *integrate* all sources of information to see the enemy as a whole. Integrated all-source analysis should also inform and shape strategies to collect more intelligence [original emphasis]" (9/11 Commission Report 2004: 401).[15] Hence, although there was enough information, it needed to be shared and properly analyzed. The second dimension is closely

[15] For further consideration, see the entirety of the Commission's discussion in section 13.3, entitled 'Unity of Effort in Sharing Information'. Additionally, the Joint Inquiry Report also has an interesting discussion of how the intelligence community "failed to capitalize on both the individual and collective significance of available information that appears relevant to the events of September 11" (Joint Inquiry Report 2002:33). This can be found in section three, entitled 'Findings and Conclusions'. Arguably this failure is closely connected to a more specific problem, namely, the difficulty of identifying meaningful patterns or relationships in vast quantities of data. "Individual data items – relating to people, places, and events, even if identified as relevant – are essentially meaningless unless viewed in context of their relation to other data points. It is the network or pattern itself that must be identified, analyzed, and acted upon" (Taipale 2003: 33). And this is precisely why DeRosa argues that data mining represents an especially promising mode of analysis which will enable intelligence agencies and law enforcement authorities to acquire the ability to 'see the enemy as a whole'. To be sure, "[t]he September 11, 2001, attacks illustrate this point. Even in hindsight, we can see no single source—other than perhaps an extraordinarily well-placed human asset—that could have provided the full or even a large part of the picture of what was being planned. We have seen a number of clues, however, that if recognized, combined, and analyzed might have given us enough to track down the terrorists and stop their plan. Therefore, although we must still focus on improving our ability to collect human and other traditional sources of intelligence, our edge now will come more from breadth of access to information and quality analysis. For counterterrorism, we must be able to find a few small dots of data in a sea of information and make a picture out of them" (DeRosa 2004: 5).

connected to the first in the following way: insofar as vast amounts of data are available for analysis, and data mining is one form of analysis amenable to the task, then pattern-based predictive data mining will simply be more effective when it is employed within large databases, as it has more data to interpret and can therefore generate a profile which is rich in information and detail.

There are at least four distinct methods by which the United States government has sought to obtain access to vast amounts of personal information: through the construction of government owned and operated data warehouses; through the development of government administered data fusion centers; through legislative measures designed to provide the government with access to private sector databases; and through partnerships with private data aggregators. Although all of these methods warrant close consideration, for the purposes of this paper only one will be discussed, namely: the use of government administered data fusion centers.

The notion of a 'fusion center' is based on the idea that disparate and relatively 'disconnected' databases, owned and operated by either the government or the private sector, can be combined or 'streamlined' in such a way that the separate databases continue to be managed by the party that constructed it, but the data which is collected by the fusion center is accessible to select individuals or actors for specific (usually classified) reasons. The (now defunct) Total Information Awareness (TIA) project is perhaps the most controversial example of a government established data fusion center. According to Peter Gill, "TIA sought to bring together in 'ultra-large all-source information repositories' a number of existing CIT programmes – identifying links from message traffic and open source data, collaborative tools

for humans and machines to 'think together', language processing for non-linguists, identification of predictive indicators of terrorist attacks, biometric identification technologies and exploiting 'nontraditional data sources to enable early detection and warning of a bioterrorist event'" (Gill 2010: 476). However, although Congress refused to continue funding for TIA (thereby effectively ending the program), other similar initiatives have been created.

A second highly controversial government initiative "intended to aggregate and analyze vast amounts of private-sector information on the activities of Americans is the MATRIX, which stands for 'Multi-State Antiterrorism Information Exchange.' Like TIA, this program is based on bringing together vast amounts of information to detect terrorism and other crimes, except the MATRIX is run at the state level, and combines government databases from participating states with a private database that claims to have '20+ billion records from 100's of sources'" (Stanley 2004: 24).[16][17] According to Seifert, "[t]he analytical core of the MATRIX pilot project was an

[16] The MATRIX project is only one of several similar government initiatives designed to enhance access to information, which in turn is only one dimension of a more comprehensive domestic counterterrorism strategy. In addition to the MATRIX Project, Seifert discusses five similar government projects introduced subsequent to 9/11. These include the Terrorism Information Awareness (TIA) project, the Computer-Assisted Passenger Prescreening System II (CAPPS II) project, the Automated Targeting System (ATS), "and data collection and analysis projects being conducted by the National Security Agency (NSA)", such as the Novel Intelligence from Massive Data (NIMD) program (Seifert 2007: II). Importantly, although TIA was cancelled by Congress, and CAPPS II was replaced in 2004 by a similar program called 'Secure Flight', all of the aforementioned programs were created after 9/11 in response to the threat of terrorism.

[17] Public-private partnerships in the area of intelligence operations, specifically the collection and analysis of data, have attracted a lot of attention after 9/11. The United States government has made efforts to exploit the potential of vast private sector databases and data analysis programs for intelligence and counterterrorism measures. For example, since 9/11 the government has introduced comprehensive agreements with private data aggregators and data collectors. Stanley claims that "[t]hese companies, which include Acxiom, Choicepoint, Lexis-Nexis and many others, are largely invisible to the average person, but make up an enormous, multi-billion-dollar industry" (Stanley 2004: 25). And according to Stanley, [o]ne of the biggest data aggregators, for example, Choicepoint, claims to have contracts with at least 35 government agencies. It has an $8 million contract with the Justice Department that allows FBI agents to tap into the company's vast database of personal information on individuals, as well as contracts with the Drug Enforcement Administration, the U.S. Marshals Service, the IRS, the Bureau of Citizenship and Immigration Services (formerly INS) and the Bureau of Alcohol, Tobacco and Firearms. Another data aggregator, Seisint Inc., has received more than $9.2 million in grant money from the Department of Justice and the Department of Homeland Security to provide commercial data to the MATRIX program (Stanley

application called Factual Analysis Criminal Threat Solution (FACTS). FACTS was described as a 'technological, investigative tool allowing query-based searches of available state and public records in the data reference repository'" (Seifert 2007: 15). More importantly,

> the data reference repository used with FACTS represented the amalgamation of over 3.9 billion public records collected from thousands of sources. Some of the data contained in FACTS included FAA pilot licenses and aircraft ownership records, property ownership records, information on vessels registered with the Coast Guard, state sexual offenders lists, federal terrorist watch lists, corporation filings, Uniform Commercial Code filings, bankruptcy filings, state-issued professional licenses, criminal history information, department of corrections information and photo images, driver's license information and photo images, motor vehicle registration information, and information from commercial sources that 'are generally available to the public or legally permissible under federal law' (Seifert 2007: 15-16).

In 2004 the United States General Accounting Office published a report entitled *Data Mining: Federal Efforts Cover a Wide Range of Uses*. In the context of a discussion pertaining to the MATRIX program, the GAO claims that MATRIX "provides the capability to store, analyze, and exchange sensitive terrorism-related and other criminal intelligence data among agencies within a state, among states, and between state and federal agencies" (GAO 2004: 5).

Although the aforementioned government initiatives, involving the use of pattern-based predictive data mining and the development of data fusion centers, are both relatively recent insofar as they have been pursued subsequent to 9/11 in response to pressure and criticism stemming from the government's perceived failure to adequately interpret and use data which could have led to the identification of the 9/11 hijackers prior to the attacks, scholars have argued that recent developments in the field of automated data analysis provide even greater

---

2005: 26). For a thorough analysis of public-private partnerships and intelligence operations in the United States, see Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*.

promise for intelligence and counterterrorism applications. According to Taipale, “current research and development efforts are aimed at developing techniques for ‘virtual’ data aggregation in which a single query or intelligent agent negotiates access to multiple distributed databases on local terms. Under this approach, instead of importing data and standardizing it for processing centrally, an intelligent ‘prospecting agent’ accesses distributed databases over a network and adapts to the local database conditions or requirements, both for database access and for data processing” (Taipale 2003: 26). For this reason, recent developments in automated data analysis suggest that, in the near future, access to, or the development of, massive data warehousing or data fusion centers will become unnecessary. However, automated data analysis also provides intelligence agencies and law enforcement authorities with the ability to engage in large scale real-time surveillance (also called ‘dataveillance’).

Perhaps one of the first examples of automated data analysis is proposed in *Active Data Mining*, by Rakesh Agrawal and Giuseppe Psaila. In this text the authors introduce what they refer to as an ‘active data mining paradigm’, whereby data is continuously mined by semi-automated systems that seek to establish patterns and predict potential outcomes based on a set of rules derived from prior data analyses. In this particular case, “[s]uch active systems can be used, for instance, to build early warning systems for spotting trends in the retail industry” (Agrawal and Psaila 1995: 3). Although the authors were writing in 1995, and although they claim their model can be used to ‘build early warning systems for spotting trends in the *retail* industry’, the potential of such a technique has not been lost on those working in the field of security and defense. In recent years there have been advances in data mining and machine learning which have spawned what are commonly referred to as ‘intelligent agents’.

According to Mark Last, "[a]n intelligent software agent is an autonomous program designed to perform a human-like function over a network or the Internet. Specifically, information agents are responsible for filtering and organizing unrelated and scattered data such as large amounts of unstructured web documents" (Last 2005: 49). Furthermore, intelligent agents are also capable of performing what is often called 'pattern matching'. In this case, predetermined predictive patterns are searched for autonomously by intelligent agents. Importantly, these agents are also able to do so in real-time. "While data mining was originally conceived of as a way of extracting hidden associations from large databases, when coupled with agent technology it can be used to monitor events, extract important information via the Internet, intranets, and other proprietary networks, discover new patterns, assemble profiles, and deliver alerts to military, medical, law enforcement, and intelligence agency personnel" (Mena 2003: 120). The possibility of using automated data analysis for real-time data mining applications is based on the development of "algorithms that improve their performance automatically through experience, such as neural networks or decision trees" (Seifert 2007: 1). Hence, "[a]gents represent a key technology to homeland security due to their capability to monitor multiple diverse locations, communicate their findings asynchronously, collaborate with each other, analyze conditions, issue real-time alerts, and profile possible threats" (Last 2005: 49).[18]

[18] Last discusses several 'agent-based systems' that are currently being developed by researchers. For example, an adaptive "multi-agent prototype system…called EVA, keeps a repository of 'user profiles' (topics of interest). Each profile is characterized by a user query (processed by a natural language processor) and a list of starting URLs that may be provided by the user or based on a domain-specific hierarchy of subject categories (such as the Yahoo! Directory). The system creates an agent leader for each profile. The agent leader generates a team of information agents that are equipped with artificial neural networks aimed at making 'relevant/non-relevant' decisions on each retrieved page…The population of agents is periodically evolved using a neuro-genetic algorithm that selects the best terms discriminating between relevant and non-relevant documents" (Last 2005: 51).

SECTION THREE

In the first section of this paper I attempted to provide a brief outline of three risk-based governmental rationalities. When doing so I focused specifically on the way that each rationality is premised on a particular conception of risk, which informs a kind of conduct that is dictated in accordance with that conception of risk. Furthermore, I also sought to provide some indication of how thinkers working within the field of critical security studies have sought to explain contemporary post-9/11 developments in the United States through recourse to either a logic of precaution or a logic of preparedness. In the second section of this paper I turned to an analysis of recent government initiatives aimed at enhancing or developing a powerful data mining capability as part of a comprehensive counterterrorism effort. To be more precise, I argued that pattern-based data mining is deployed in order to predict potential terrorist threats by analyzing vast quantities of data so as to identify patterns which correspond to either predetermined models of terrorist activity or deviate from the expected norm of what 'usual' or 'common' behavior ought to be. In addition, though (and perhaps more importantly), researchers have developed techniques whereby pattern-based data mining can be performed autonomously by 'intelligent agents', which are capable of mining both structured and unstructured data in real-time. The potential contribution of these applications for domestic surveillance operations aimed at identifying terrorists or potential terrorist activities is immense, and it is for precisely this reason that several government departments and agencies have sought to support additional research into such data mining techniques and the deployment of these applications.

As we have seen, the use of pattern-based predictive data mining for domestic counterterrorism surveillance operations is closely connected to the problem of detecting and preventing a terrorist attack in the United States. In particular, the risk posed by the threat of terrorism introduces an imperative which dictates or necessitates a certain form of practice capable of providing law enforcement authorities and intelligence agencies with the ability to effectively pre-empt the risk before it materializes. This is why Aradau and van Munster argue that, in the post-9/11 age, "[p]recautionary risk management implies the surveillance of all the population, of all flights for example, independent of existing intelligence. Hence more and more technologies of surveillance are indiscriminately targeted at the whole population: stop and search policies in the UK, biometric identifiers or the introduction of identity cards" (Aradau and van Munster 2007: 115). Their argument revolves around the way that 'uncertainty' has come to increasingly inform counterterrorism policy, planning, and strategy as it is developed within governmental departments and agencies. The problem of uncertainty has been expressed by senior government officials and intelligence experts, and at its most extreme it entails that officials can never be sure that there is not an individual (a 'lone wolf') or group of individuals currently planning or preparing for a terrorist attack. Uncertainty – which in precautionary thinking functions as the limit of knowledge – thereby necessitates the acquisition of more knowledge. Post-9/11 developments in domestic surveillance, according to Aradau and van Munster, represent one solution to this problem.

Although there may be good reason to believe that 'more and more technologies of surveillance are indiscriminately targeted at the whole population' (which is inevitable given the rather peculiar and unique problem raised by the threat of terrorism – i.e., the problem

highlighted by Pillar), it is not clear that this development in the field of domestic surveillance is 'implied' by the logic of precautionary risk management. In particular, it is not clear that pattern-based predictive data mining, understood here as one particular technique of domestic counterterrorism surveillance practice, is a manifestation of precautionary risk management. While this represents a crucial problem for Aradau and van Munster, I argue that the use of pattern-based predictive data mining for domestic counterterrorism surveillance cannot be rendered intelligible as a technology of either insurance or preparedness. Thus, if I am correct, *none* of the aforementioned risk-based governmental rationalities can adequately explain this critical development in the field of post-9/11 security practice.

In the following discussion I intend to do three things. First, I will demonstrate why pattern-based predictive data mining for domestic counterterrorism surveillance operations cannot be adequately explained through recourse to the three risk-based rationalities of insurance, precaution, or preparedness. In addition, because Aradau and van Munster argue that precautionary thinking implies certain forms of contemporary state surveillance, and that these can therefore be explained through recourse to a precautionary approach, my position is clearly at odds with that of Aradau and van Munster. Therefore I will offer at least one possible explanation as to why Aradau and van Munster are incorrect in their analysis. Second, I argue that if pattern-based data mining is utilized for domestic counterterrorism surveillance, it is to be understood as a form of surveillance practice which is tailored in accordance with a specific conception of risk. More importantly, the fact that it cannot be explained through recourse to the other risk-based rationalities outlined in the governmentality literature suggests that there is a fourth risk-based governmental rationality which needs to be elucidated. I claim that this

rationality seems to operate according to the logic of risk pre-emption. Third, I then discuss several considerations pertaining to the direction of future research into a governmental rationality of risk pre-emption.

The question of whether pattern-based predictive data mining and its use as a technology of domestic counterterrorism surveillance practice can be explained through recourse to either a rationality of insurance, precaution, or preparedness, depends in large part on the extent to which the specific conceptions of risk on which these risk-based rationalities are premised corresponds to that which pattern-based predictive data mining is intended to address.

If the reader recalls, according to Ewald there are three general characteristics of insurance risk. First, risk is calculable and is thereby assigned a certain degree of probability. In this way, it is rendered 'objective' and can become the object not only of thought, but also of insurance practice. Second, insurance risk is collective, which is to be understood in two distinct though closely related ways. On the one hand, risk is viewed as a naturally occurring phenomenon which is inherent to a given population. On the other hand, and for precisely this reason, it is also something which can only effect the population as a whole. "Strictly speaking there is no such thing as an individual risk; otherwise insurance would be no more than a wager" (Ewald 1991: 203). And third, risk is treated as a 'capital', meaning that some form of monetary remediation is conceivable. This is why Ewald claims that "[o]ne and the same event acquires a dual status: on the one hand, a happening with the uniqueness of the irreparable; on the other, an indemnifiable risk" (Ewald 1991: 204).

It is clear that one of the primary reasons as to why intelligence agencies and law enforcement authorities have supported initiatives aimed at utilizing pattern-based predictive data mining for domestic counterterrorism surveillance operations is to prevent the possibility of a future terrorist attack. Indeed, arguably this holds true when considering any counterterrorism measure. But as we have seen, technologies of insurance do not make any attempt to prevent the occurrence of a risk. Rather, it is assumed that certain forms of risk are inevitable; that they will transpire and inflict some kind of damage regardless of what is done to avoid such an outcome. Therefore all that can be done is to compensate the unfortunate person who happens to experience the undesirable consequences. Hence, it is difficult to reconcile these two conceptions of risk: that of insurance as it is outlined by Ewald, and the risk posed by the threat of terrorism. Consequently, it is equally difficult to view pattern-based predictive data mining as a technology of insurance practice.

When considering whether or not pattern-based predictive data mining is a form of domestic surveillance practice which can be explained by viewing it as a particular form of conduct which operates in accordance with the logic of preparedness (as it was outlined by Lakoff), there is at least one important point to bear in mind. Although certain government departments, such as the Department of Defence, the Department of Homeland Security, and virtually all police departments, fire departments, and first responders, devote (in some cases substantial) resources to emergency planning and disaster recovery, this does not represent the only way in which government departments and agencies address the risk posed by the threat of terrorism. That is to say, they are not simply concerned with mitigating the disastrous effects of a bioterrorist attack on some piece of infrastructure deemed to be ‘critical’ to national

security and safety. As we have seen, they also fund and support programs or other initiatives aimed at *preventing* the occurrence of a possible attack. Hence, one and the same institution or agency may develop policies, fund research, or introduce, as part of its mandate, measures which are premised on the need to prepare for an eventual catastrophe, *as well as* preventive measures designed to ensure that *other* forms of catastrophe *never* materialize and threaten the security of the state.

This is especially interesting, for it suggests that even though Lakoff was not entirely wrong, the focus with which he had to pursue his analysis ensured that he could not explore other avenues, i.e., those that would have led him to the conclusion that at least two risk-based governmental rationalities may inform the policies, procedures, and operations of a single government agency. This raises the possibility that at least one other risk-based governmental rationality may actually be operating in tandem with that of preparedness. Clearly and precisely establishing this dynamic is no doubt a difficult task, but it could help to resolve a rather peculiar problem that is addressed in the context of Lakoff's analysis, namely: "how a series of seemingly disparate types of events — ranging from terrorist attacks, to hurricanes and earthquakes, to epidemics — have been brought into the same framework of 'security threats'" (Lakoff 2007: 247). Insofar as state-based security practices are indeed operating within a socio-political environment characterized, at least in part, by the fact that just about anything can be deemed a potential security threat, perhaps this is best explained by viewing this development as informed not by a single logic of 'preparedness', but by seeing (at least) two distinct risk-based rationalities affecting the determination of security threats at precise moments within disparate contexts.

This brings us to the question of the extent to which pattern-based predictive data mining, and its use for domestic counterterrorism surveillance by intelligence agencies and law enforcement authorities, reflects the logic of precautionary thinking. In their article, Aradau and van Munster claim that certain post-9/11 developments in surveillance demonstrate that precautionary thinking has informed the conduct of domestic surveillance operations. The authors then proceed to flesh out some of the implications that this may have for our understanding of how dissimilar developments unique to the 'war on terror' are 'governed' or informed by the notion of 'precautionary risk'. In particular, Aradau and van Munster argue that "[t]he dispositif of risk as a heterogeneous assemblage of discursive and material elements [in contrast to "practices of proactive risk management as analysed by Didier Bigo" and Ulrich Beck's understanding of terrorism as "another manifestation of 'world risk society'" (Aradau and van Munster 2007: 91)] will enable us to locate developments as diverse as the wars in Afghanistan and Iraq, the targeting of Muslim communities by counter-terrorism measures or indefinite detention of suspect terrorists in the UK as elements of precautionary governance through risk. Rather than bellicose decisions or arbitrary executive measures, these different policies will be shown to function within a dispositif of precautionary risk" (Aradau and van Munster 2007: 94).

There are several reasons as to why it would appear as though pattern-based predictive data mining and its use for domestic counterterrorism surveillance operations is indeed a distinct security practice which functions 'within a dispositif of precautionary risk'. The risk posed by the threat of terrorism can be catastrophic (in the sense that it can cause irreparable and irremediable harm), it is incalculable (in the sense that one cannot accurately predict the

probability of its occurrence), it is 'man-made', and it is not inevitable. Arguably, then, it would appear as though the risk of a potential terrorist attack can be prevented by implementing measures in accordance with the precautionary principle insofar as the specific kind of risk that terrorism is (or is represented as) seems to be consistent with that which precautionary thinking is premised on. This appears to be why Aradau and van Munster argue that "[p]recautionary risk management implies the surveillance of all the population, of all flights for example, independent of existing intelligence. Hence more and more technologies of surveillance are indiscriminately targeted at the whole population: stop and search policies in the UK, biometric identifiers or the introduction of identity cards" (Aradau and van Munster 2007: 27).

Several authors have pointed out that the post-9/11 age has seen a dramatic expansion of state surveillance, and to such an extent that now contemporary surveillance indiscriminately targets the whole population. While this is controversial (from the perspective of a legal, ethical, and political standpoint), it is not a particularly novel claim to make. However, what is interesting about this claim is that it seems to discount the possibility that there are forms of surveillance practice which do not operate in accordance with the logic of precautionary risk management. Hence, on the basis of Aradau and van Munster's argument, all forms of state surveillance practice in the post-9/11 function 'within a dispositif of precautionary risk'. By extension, then, the use of pattern-based predictive data mining by intelligence agencies and law enforcement authorities engaged in domestic counterterrorism surveillance can only be properly understood if it is situated 'within a dispositif of precautionary risk'.

To what extent, though, is it correct to make such a claim? The answer to this question depends on how one answers the following question: To what extent is the particular notion of precautionary logic elaborated by Aradau and Munster consistent with Ewald's analysis? For Aradau and van Munster ground much of their discussion regarding the logic of precaution on Ewald's analysis of the precautionary principle. Importantly, I contend that there is at least one important difference that needs to be discussed.

As we have seen, Ewald maintains that precautionary thinking holds out the possibility of risk prevention by positing a probable (loosely causal) relationship between a given action or set of actions and the materialization of a potential risk, where the latter is understood to be an effect or consequence of the action *qua* cause. In this sense, then, the relationship between act and risk is one which, though not clearly identifiable from the standpoint of the actor who engages in the act, is nevertheless one which highlights the fact that, if the act were not performed, there is virtually no way that the risk could exist as such. By taking precautions, one essentially eliminates the potential risk. Therefore, the kind of action that is required by precautionary thinking demands that an individual or group refrain from engaging in actions that may possibly involve a (loosely causal) relationship with the potential risk. Precaution, then, demands that one *not* engage in certain actions on the grounds that those actions may lead to irreversible and irreparable damage.

But on the basis of our previous discussion of pattern-based predictive data mining, it would be difficult to maintain that this particular technique of domestic counterterrorism surveillance operates in accordance with a precautionary logic. Although surveillance undoubtedly has an effect on behavior and thus would seem to represent a form of behavior

modification intended to ensure that a potentially dangerous risk resulting from the execution of a given act or set of actions does not materialize, if one is to maintain that this demonstrates or reflects the influence of precautionary thinking one would then have to show how surveillance is a preventative measure undertaken by those who, if they did not engage in surveillance, are likely to 'cause' a terrorist attack. Thus, it appears as though Aradau and van Munster may have taken any kind of preventive measure intended to reduce or eliminate the occurrence of a potentially catastrophic risk as an instantiation of precautionary risk management.

If pattern-based predictive data mining operates on the basis of an entirely different logic (one that is to be distinguished from insurance, precaution, or preparedness), and if we have good reason to believe that this technique of domestic counterterrorism surveillance is orientated by an altogether different conception of risk (one which is to be distinguished from those found in insurance, precaution, or preparedness), this represents an important new direction in research on the connection between the threat of terrorism *qua* risk, post-9/11 state security practice, and the associated rationalities which render such practices intelligible. For the remainder of this discussion, I will offer several general remarks on how future research might proceed.

To begin with, it is clearly necessary to delineate the general contours of a risk-based rationality premised on the *pre-emption* of risk. A risk-based rationality which informs a set of practices orientated by the pre-emption of risk is reflective of an altogether unique conception of risk, for it is the ontological peculiarity of the risk in question which calls for or necessitates practices that make possible the pre-emption of risk. As a preliminary attempt to establish the

contours of this particular conception of risk, we will say that it has the following characteristics.

First, like the forms of risk addressed by precautionary thinking and preparedness, the risk posed by the threat of terrorism is treated as catastrophic, i.e. as that for which there can be no compensation or remediation. This is what necessitates the adoption of a 'zero-risk' threshold and justifies the implementation of surveillance practices and programs that transgress conventional limitations pertaining to traditional fundamental rights and freedoms. This also represents a crucial difference between pre-emptive risk and insurance risk. It is precisely the fact that pre-emptive risk cannot be rendered familiar, that it cannot be normalized, which means that the persistence of the risk posed by the threat of terrorism pushes surveillance (security) practice into the realm of the exceptional.

Second, unlike precautionary risk, pre-emptive risk is not 'caused', either directly or indirectly, by an actor who is willing to modify their behavior in order to avert the impending catastrophe. Lakoff clearly elaborates the rationale behind every injunction issued by the precautionary principle when he writes: "a principle of precaution in the face of an incalculable threat enjoins against risk-taking — for example, the implementation of new and uncertain technologies such as genetically modified food. In this manner, it seeks to keep the dangerous event from occurring" (Lakoff 2007: 253). The precautionary principle is able to enjoin against risk taking only when the risk taking can be averted by the actor originally compelled to engage in risky behavior. Hence, pre-emptive risk cannot necessitate anything like the precautionary principle.

Third, pre-emptive risk is avoidable and is certainly not inevitable. Indeed, this is precisely what makes the pre-emption of such risk possible. In this sense, pre-emptive risk is similar to precautionary risk though different from the risk of insurance and preparedness (where the latter calls for the implementation of measures designed to mitigate or alleviate the consequences of a potential catastrophe). Furthermore, and perhaps more importantly, because pre-emptive risk can be prevented from materializing, it is always treated in terms of an existant potentiality, which has a reality that is not, strictly speaking, identical with its materialization (for this would mean that the potential risk is identical with the risk in question). Rather, pre-emptive security practices always intervene in the present against some potentiality which threatens to materialize and become a risk (a threat). Hence, in terms of its intelligibility, the risk posed by the threat of terrorism is to be understood in terms of an imagined reality, though insofar as the pre-emption of this risk operates on the level of potentiality, we must say that it is the potentiality which is given to thought as something that is intelligible and known. For this reason, although the risk posed by the threat of terrorism can never be objectively known, the potentiality of that risk can be.

Fourth, although it is possible to imagine cases where the specifics of a terrorist plot cannot be known in advance, pattern-based data mining treats the risk of a terrorist attack as something which may be predicted. As we have already seen, there are two different ways by which this occurs. The first involves searching for a predetermined ‘model’ or pattern throughout extensive databases. If the data inquiry discovers a ‘match’, law enforcement authorities apprehend the individual or conduct further, more extensive investigations with the aim of ascertaining whether or not a plot really is being hatched. The second method occurs in

real-time and is not necessarily concerned with discovering a pre-determined pattern in the data so much as alerting authorities to the fact that a given individual is *currently* engaging in acts which are cause for suspicion. Hence, we must differentiate the precise manner by which pre-emptive risk is predicted: in contrast to insurance, which establishes "the objective probability of an accident" and therefore also the fact that "accidents occur at a particular, specific rate" (Ewald 1991: 202), practices orientated by the pre-emption of risk are predictive in the sense that they identify a number of conditions which are deemed likely to lead to an imagined and pre-determined result. Arguably there is still an element of probability involved in practices of pre-emptive risk, but there is a sense in which this instantiation of probability is not generated through statistical calculation.

This has a number of interesting implications, not least of which concerns the practice of imagining potential terrorist 'activities' or 'behaviors' in order to effectively model and thereby identify (prior to the occurrence of a terrorist attack) the individual engaged in preparing for such an attack. In *Beyond Risk: Premediation and the Post-9/11 Security Imagination*, Marieke De Goede argues that 'premediation', a term initially used to "describe the way in which news media and cultural industries map out 'as many of the possible worlds, or possible paths, as the future could be imagined to take'", designates a critical function of post-9/11 security discourse and now characterizes a variety of post-9/11 security practices (De Goede 2008: 156). Furthermore, although De Goede is interested in drawing a distinction between the 'logic of risk' and that of premediation, such that "the logic of risk and forecasting centres on *prediction* of the future, [whereas] premediation is more self consciously 'creative' in imagining a variety of futures – some thought likely, others far-fetched, some thought imminent, others long-haul

– in order to *enable action in the present*" (De Goede 2008: 159), this distinction may hold only on condition that one accepts that there is a single 'logic of risk'.[19]

It is not clear as though premediation exceeds either the logic of preparedness or the logic of risk pre-emption. In fact, De Goede's discussion of premediation and its role in contemporary security discourse and practice has a lot to contribute to an analysis of how the logic of risk pre-emption is entirely consistent with, and indeed, perhaps depends upon, the logic of premediation. Of particular interest is the idea that "premediation is not about the future *at all*, but about enabling action in the present by visualizing and drawing on multiple imagined futures" (De Goede 2008: 159). This is interesting insofar as it points towards one technique by which the pre-emption of risk is facilitated: one may establish a model of a possible future by imagining that future and the conditions of its possibility. As we have seen in our discussion of pattern-based predictive data mining, the use of models, or specific configurations of data 'items' deemed significant, is a common and often effective method employed in order to identify, even in real-time, individuals who may be planning to carry out a terrorist attack.

A final point I would like to raise concerns what might be called the 'origin' or history of a risk-based rationality premised on the logic of risk pre-emption. The reader may recall that

[19] At times it appears as though the 'logic of risk calculation' and 'risk management' that De Goede has in mind are those often (if not entirely) practiced within insurance. Consider the following: "practices of premediation exceed the logic of risk calculation and self-consciously deploy imagination in their scenarios, worst-case narratives and disaster rehearsals" (De Goede 2008: 156). Hence, we may say that premediation exceeds the logic of risk calculation as it is practiced in insurance. That being said, in the immediate context of the article De Goede is primarily concerned with techniques of risk management deployed in the 'war on terror', and it would be difficult to maintain that these techniques, which are exceeded by practices of premediation, are those deployed by insurance. Indeed, it is doubtful that De Goede would be committed to the view that practices of insurance are deployed as forms of risk management in the war on terror. On the other hand, the self-conscious deployment of imagination in 'scenarios, worst-case narratives and disaster rehearsals' characterizes emergency preparedness, which is a risk-based rationality that, as Lakoff argues, does not privilege the same methods of risk calculation as does insurance.

Ewald identifies the origin of insurance at what is essentially a convergence of several conditions, such as the development of a rigorous statistical method, the industrialization of labor and the emergence of industrial accidents as a cost that employers needed to guard themselves against, as well as a more general reformulation of principles of justice and legal right (Ewald 1991: 204-206). In a particular socio-economic, political, and cultural context, a number of general developments, each with a trajectory that seems to trend in a similar direction, converged in such a way that insurance could be rendered intelligible as a particular technology with which to manage or govern risk. Similarly, Ewald locates the origin of the precautionary principle in international, regional, and municipal legal regimes which had emerged during the 1980's in order to address environmental degradation, transnational health pandemics, and the liability of products manufacturers. Furthermore, Lakoff also attempts to locate the emergence of preparedness, and argues that "[w]hile techniques of preparedness are now applied to a variety of potential disasters, they were initially assembled in the Cold War United States, in response to the threat of a surprise nuclear attack by the Soviet Union" (Lakoff 2007: 255).

In all three cases an attempt has been made to explain the origin and development of the risk-based rationality and many associated practices. If there is indeed a fourth risk-based rationality premised on the logic of risk pre-emption, it is reasonable to assume that, like insurance, precaution, and preparedness, it would also have a history and a point of origin. And although it no doubt precedes the emergence of pattern-based predictive data mining and its use for domestic counterterrorism surveillance, in this paper there has been no effort at identifying the specific socio-economic, political, cultural, and institutional conditions which

gave rise to a rationality of risk pre-emption. Admittedly this represents a significant limitation to the general argument which had developed in the context of this paper. Here it is important to raise one final point.

The question as to when the pre-emption of risk emerged as a unique governmental rationality is important. Although it is beyond the scope of this paper to address the question here, it must be kept in mind that the terms ‘pre-emption’ and ‘pre-empt’ are extremely loaded and are being used, here, in a merely tentative manner so as to capture the basic dynamic of this more general approach to risk. It is imperative that one does not allow the connotations and associations of the term itself to mislead or otherwise confuse the frame within which any future inquiry is conducted. For the term appears in a number of diverse contexts throughout history and may even outdate insurance, precaution, and preparedness.

CONCLUSION

In this paper I have sought to demonstrate that the use of pattern-based predictive data mining, by intelligence agencies and law enforcement authorities, for domestic counterterrorism surveillance operations, is not a form of surveillance practice that can be explained through recourse to the three risk-based governmental rationalities which have already been outlined and, in the case of precaution and preparedness, have informed analyses conducted by scholars working in the field of critical security studies. Although this may, at first glance, suggest that the concepts, principles, and general analytical perspective offered by governmentality studies do not provide a fertile source for analyzing and explaining the application of pattern-based predictive data mining to post-9/11 domestic counterterrorism surveillance operations, I argue that this is not the case. Rather, instead of thinking about this form of surveillance practice as a manifestation of one of the aforementioned risk-based rationalities, there is good reason to view it as a form of security practice which is informed by a rationality and logic of risk pre-emption.

If it is correct to claim that there is indeed a fourth risk-based rationality, which has not been previously discussed or examined in the governmentality literature, this possibility raises a number of questions and opens up a promising direction for future research into governmental rationalities in general, and the way that certain forms of contemporary post-9/11 security practice operate, in particular. In this paper I have attempted to offer what are merely preliminary remarks in order to delineate the general contours of pre-emptive risk, and I have done so by differentiating this particular notion of risk from those of insurance, precaution, and preparedness.

This (albeit preliminary) exposition of pre-emptive risk in no way presumes that precautionary or preparedness thinking are irrelevant when seeking to understand contemporary developments in post-9/11 state security practice. Indeed, despite the fact that Lakoff did not account for the possibility that one and the same institution – whether this be the Department of Homeland Security or the Department of Defence – could actually adopt (at least) two distinct though complementary risk-based rationalities and simultaneously engage in various forms of practice consistent with these rationalities, his analysis still sheds much needed light on an important and promising development in critical security studies (i.e., "the emergence and extension of 'preparedness' as a form of rationality for approaching questions of domestic security in the United States" [Lakoff 2007: 247])

Similarly, even if their appropriation of Ewald's work on the precautionary principle overlooked several crucial considerations, which therefore explains why pattern-based predictive data mining represents a difficult problem for their argument, the idea that a precautionary approach to risk management has come to inform a number of disparate security practices subsequent to 9/11 is promising. That being said, in order to effectively situate post-9/11 security practice within a dispositif of precautionary risk, one would have to show how the United States, for example, seeks to reduce or eliminate the risk posed by the threat of terrorism by *refraining* from risky behavior, where there is a possibility that such behavior would lead to the risk in question. Perhaps one place where an example of this could be located is in the 'hearts and minds' discourse and practice which has become a decisive component of counter-insurgency operations in the war on terror.

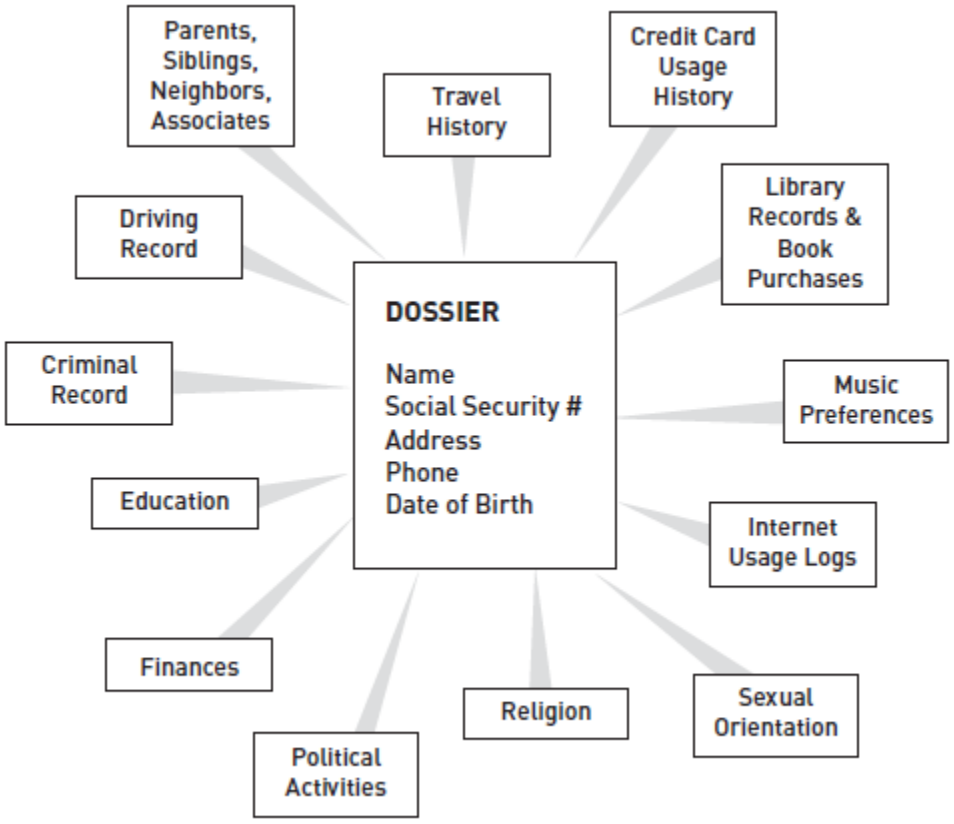
Of particular interest is the possibility that one peculiar technology of pre-emptive risk is a technique described by De Goede as premediation. While De Goede argues that "practices of premediation exceed the logic of risk calculation and self-consciously deploy imagination in their scenarios, worst-case narratives and disaster rehearsals" (De Goede 2008: 156), this line of argument may hold only if the 'logic of risk calculation' that De Goede has in mind is that of insurance. However, if De Goede is open to the idea that there are several distinct forms of risk which dictate or necessitate varying ways of thinking about risk (i.e., of imagining, calculating, rationalizing, or otherwise construing risk), then it would seem as though practices of premediation may not only exceed the logic of insurance, but are also a crucial technology of preparedness and pre-emptive risk. According to the author, practices of premediation (and specifically the practice of deploying imagination in the development of scenarios) "respond to the 9/11 Commission's call for scenario testing and are thought to enable the *preemption* of security threats [original emphasis]" (De Goede 2008: 156). This suggests that there is actually a strong connection between the emergence of a rationality of risk pre-emption, and the institutionally recognized need for practices of premediation.

This brings us to the question of how to properly elucidate the origin of the rationality of risk pre-emption, including of course a sustained consideration of the socio-economic, political, and cultural conditions which facilitated the emergence of this peculiar rationality and made it possible for its principles to become inscribed in institutions capable of determining consistent forms of conduct, or practice. Importantly, any inquiry into the origin of risk pre-emption must guard against confusing traditional instantiations of what are typically recognized as instances of pre-emption, as in the case of pre-emptive war, so as to ensure that one does not mistake

something like a pre-emptive war for a case of the pre-emption of risk. This is not to say that military strategy involving the use of a pre-emptive strike does not 'share' something with a rationality of risk pre-emption, but much work needs to be done in order to demonstrate conclusively that this is or is not the case.

In conclusion, provided that research in governmentality studies offers something promising for IR scholars interested in explaining contemporary developments in security practice, and provided there is good reason to believe that certain areas of domestic security practice are 'governed' or informed by a rationality of risk pre-emption, then further research into this possibility is warranted and, indeed, necessary in order to properly elucidate these developments and understand their trajectory.

APPENDIX A



From: Stanley 2004: 23

APPENDIX B

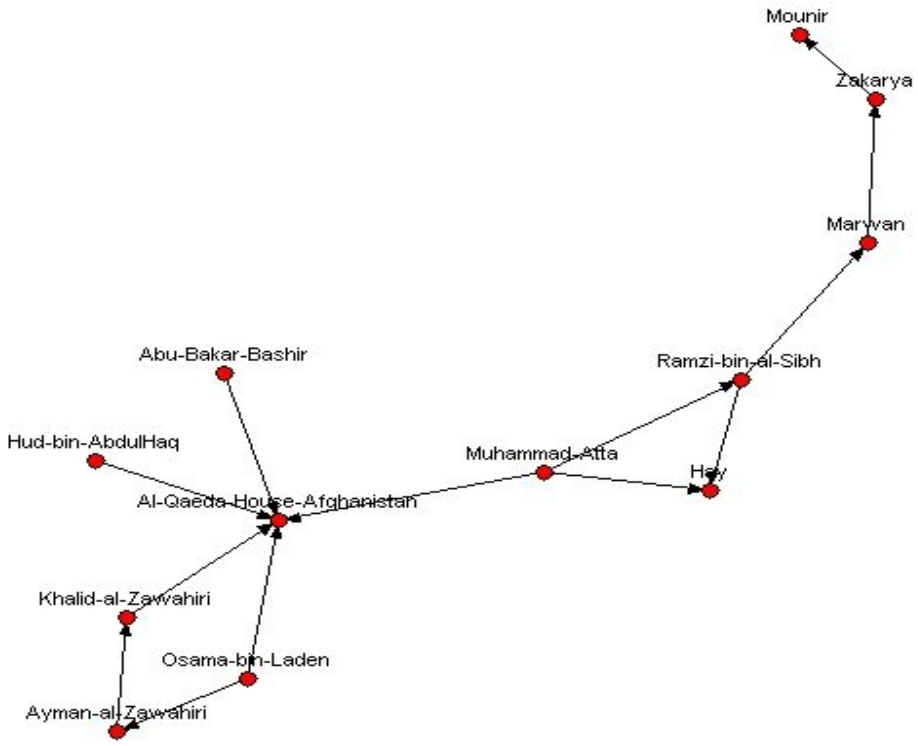


Fig 1: The connection between a set of people displayed as a network
From: Memon and Qureshi 2005: 397

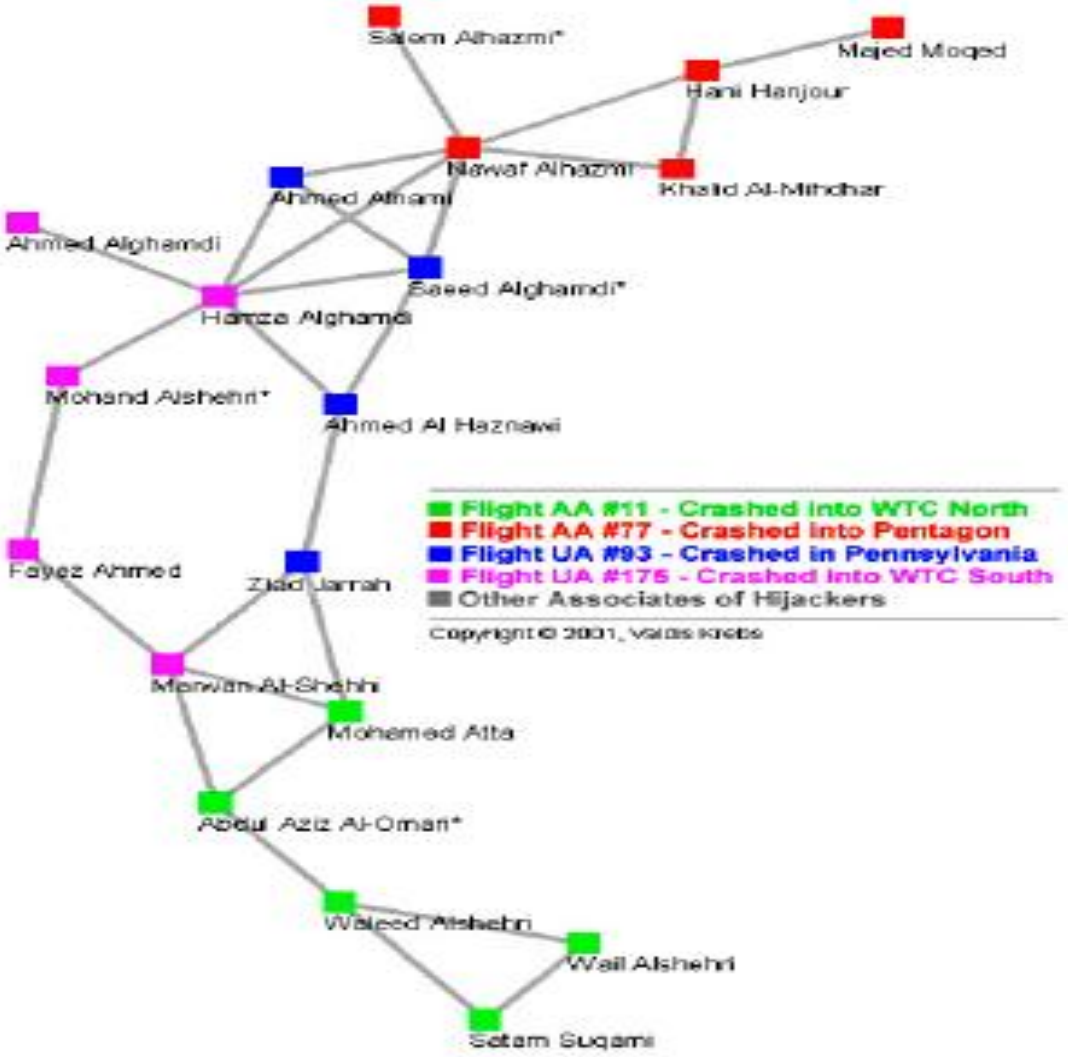


Fig. 2: 9-11 Terrorist Network
From: Memon and Qureshi 2005: 400

WORKS CITED

Agrawal, Rakesh and Giuseppe Psaila. Active Data Mining. San Jose: IBM Almaden Research Center, 1995. <https://www.aaai.org/Papers/KDD/1995/KDD95-001.pdf>. (Accessed April 30th 2012).

Amoore, Louise and Marieke De Goede. "Governance, Risk and Dataveillance in the War on Terror." Crime, Law & Social Change. Vol. 43:2 (2005): 149-173.

Aradau, Claudia and Rens van Munster. "Governing Terrorism Through Risk: Taking Precautions, (un)knowing the Future." European Journal of International Relations. Vol. 13:1 (2007): 89–115.

Beck, Ulrich. The Risk Society: Towards a New Modernity. London: SAGE Publications Ltd., 1992.

Burchell, Graham. "Liberal Government and Techniques of the Self." Economy and Society. Vol. 22:3 (1993): 267-282.

Cate, Fred H. "Government Data Mining: The Need for a Legal Framework." Harvard Civil Rights – Civil Liberties Law Review. Vol. 43:2 (2008): 435-489.

Chen, Ming-Syan, Jiawei Han, and Philip S. Yu. "Data Mining: An Overview from a Database Perspective." IEEE Transactions on Knowledge and Data Engineering. Vol. 8:6 (1996): 866-883.

Collier, Kenneth, Bernard Carey, Ellen Grusy, Curt Marjaniemi, and Donald Sautter. A Perspective on Data Mining. Northern Arizona University: The Center for Data Insight, 1998. <http://insight.nau.edu/downloads/dm%20perspective%20v2.pdf>. (Accessed April 30th 2012).

De Goede, Marieke. "Beyond Risk: Premediation and the Post-9/11 Security Imagination." Security Dialogue. Vol. 39:2-3 (2008): 155-176.

DeRosa, Mary. Data Mining and Data Analysis for Counterterrorism. Washington: The CSIS Press, 2004. <https://www.cdt.org/security/usapatriot/20040300csis.pdf>. (Accessed April 26th 2012).

Elovici, Yuval. "TDS – An Innovative Terrorist Detection System." Fighting Terror in Cyberspace. Eds. Mark Last and Abraham Kandel. Hackensack: World Scientific Publishing Co., 2005. 75-90.

Ewald, Francois. "Insurance and Risk." The Foucault Effect: Studies in Governmentality – With Two Lectures by and an Interview with Michel Foucault. Eds. Graham Burchill, Colin Gordon, and Peter Miller. Chicago: University of Chicago Press, 1991. 197-210.

Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. "From Data Mining to Knowledge Discovery in Databases." AI Magazine. Vol. 17:3 (1996): 37-54.

---. "The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution." Trans. Stephen Utz. Embracing Risk: The Changing Culture of Insurance and Responsibility. Eds. Tom Baker and Jonathon Simon. Chicago: The University of Chicago Press, 2002. 273-301.

Gill, Peter. "Securing the Globe: Intelligence and the Post-9/11 Shift from 'Liddism' to 'Drainism'." Intelligence and National Security. Vol. 19:3 (2004): 467-489.

Gordon, Colin. "Governmental Rationality." The Foucault Effect: Studies in Governmentality – With Two Lectures by and an Interview with Michel Foucault. Eds. Graham Burchill, Colin Gordon, and Peter Miller. Chicago: University of Chicago Press, 1991. 1-52.

Hacking, Ian. The Taming of Chance. New York: Cambridge University Press, 1990.

Hand, David, Heikki Mannila, and Padhraic Smyth. Principles of Data Mining. Cambridge: The MIT Press, 2001. <ftp://po.istu.ru/public/docs/other/New/Books/Misc/Principles%20of%20Data%20Mining.pdf>. (Accessed May 30th 2012).

Jonas, Jeff and Jim Harper. "Effective Counterterrorism and the Limited Role of Predictive Data Mining." Policy Analysis. No. 584 (2006): 1-12.

Lakoff, Andrew. "Preparing for the Next Emergency." Public Culture. Vol. 19:2 (2007): 247-271.

Last, Mark. "Using Data Mining Technology for Terrorist Detection on the Web." Fighting Terror in Cyberspace. Eds. Mark Last and Abraham Kandel. Hackensack: World Scientific Publishing Co., 2005. 41-62.

Lyon, David. Surveillance After September 11. Oxford: Blackwell Publishing Ltd., 2003.

Memon, Nasrullah and Abdul Rasool Qureshi. "Investigative Data Mining and Its Application in Counterterrorism." Proceedings of the 5th WSEAS International Conference on Applied Informatics and Communications. (September 2005): 397-403. <http://www.wseas.us/e-library/conferences/2005malta/papers/498-776.pdf>. (Accessed July 15th 2012).

Mena, Jesús. Investigative Data Mining for Security and Criminal Detection. Burlington: Elsevier Science, 2003.

Michaels, Jon D. "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror." California Law Review. Vol. 96:4 (2008): 901-966.

National Commission on Terrorist Attacks Upon the United States. The 9/11 Commission Report. (July 2004) <http://www.9-11commission.gov>. (Accessed February 26th 2012).

O'Malley, Pat. "Governmentality and Risk." The University of Sydney Law School: Legal Studies Research Paper No. 9. (September 2009) <http://ssrn.com/abstract=1478289>. (Accessed December 8th 2011).

Oh, JungHwan, JeongKyu Lee, and Sanjaykumar Kote. "Real Time Video Data Mining for Surveillance Video Streams." Lecture Notes in Computer Science. Vol. 2637 (2003): 566-577.

Pillar, Paul. "Counterterrorism After Al Qaeda." The Washington Quarterly. Vol. 27:3 (2004a): 101-113.

---. "Intelligence." Attacking Terrorism: Elements of a Grand Strategy. Eds. Audrey Kurth Cronin and James M. Ludes. Washington: Georgetown University Press, 2004b. 115-140.

Posner, Richard A. Catastrophe: Risk and Response. New York: Oxford University Press, 2004.

Rose, Nikolas. "The Politics of Life Itself." Theory, Culture & Society. Vol. 18:1 (2001): 1-30.

Rose, Nikolas, Pat O'Malley, and Mariana Valverde. "Governmentality." Annual Review of Law and Social Science. Vol. 2 (2006): 83-104.

Rubinstein, Ira S., Ronald D. Lee, and Paul M. Schwartz. "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches." The University of Chicago Law Review. Vol. 75:1 (2008): 261-285.

Seifert, Jeffrey W. "Data Mining and Homeland Security: An Overview." CRS Report for Congress. Washington: Congressional Research Service, 2007. <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA475315>. (Accessed May 1st 2012).

Slobogin, Christopher. "Government Data Mining and the Fourth Amendment." The University of Chicago Law Review. Vol. 75:1 (2008): 317-341.

Solove, Daniel J. "Data Mining and the Security-Liberty Debate." The University of Chicago Law Review. Vol. 75:1 (2008): 343-362.

Stanley, Jay. The Surveillance Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society. New York: The American Civil Liberties Union, 2004. <http://www.aclu.org/FilesPDFs/surveillance_report.pdf>. (Accessed April 26th 2012).

Taipale, K. A. "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data." The Columbia Science and Technology Law Review. Vol. 5:2 (2003): 1-83.

The U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence. Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001. (December 2002) <http://www.fas.org/irp/congress/2002_rpt/911rept.pdf>. (Accessed May 5th 2012).

Thuraisingham, Bhavani. "Data Mining for Counterterrorism." Data Mining: Next Generation Challenges and Future Directions. Eds. Hillol Kargupta, Anupam Joshi, Krishnamoorthy Sivakumar, and Yelena Yesha. Cambridge: The MIT Press, 2004. 157-183.

United States General Accounting Office. Data Mining: Federal Efforts Cover a Wide Range of Uses. (May 2004) <http://www.gao.gov/new.items/d04548.pdf>. (Accessed May 9th 2012).

Whitaker, Reg. "A Faustian Bargain? America and the Dream of Total Information Awareness." The New Politics of Surveillance and Visibility. Ed. Kevin D. Haggerty and Richard V. Ericson. Toronto: University of Toronto Press, 2006. 141-170