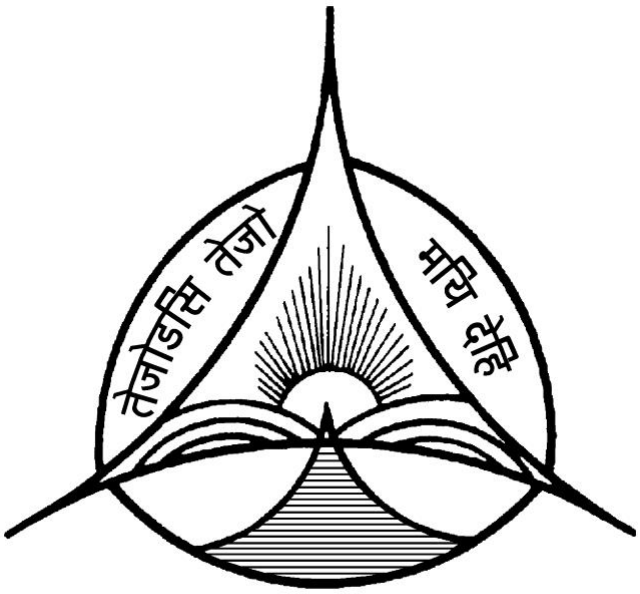
THE JMC REVIEW

An Interdisciplinary Social Science Journal of Criticism, Practice and Theory



Volume 2

2018

Security as Risk Management: Emerging Dynamics of United States Homeland Security

SHAILZA SINGH*

The global war on terror launched by the United States of America has unleashed a whole array of interventions that attempt to reinterpret our understandings of the world. One such intervention has been the transfusion of the concept of 'risk' into the domain of security. While risk as an operating principle has been a feature of financial and insurance industries, its application to various sectors of governance, determining the nature of policies, is a 21st century development. Risk management-based approaches triggered by technological advancement have pervaded governance practices worldwide, including a fast-emerging understanding of security through the risks framework.

This paper seeks to provide a general overview of the application of a risk-based approach to security in the recent past, particularly after the 9/11 terrorist attacks, through the discussion of the case of homeland security in the US. It places the discussion in the larger discourse in security studies about the nature of risk-based understanding of security and its implications. Descriptive analytical method is applied to both primary sources (which include publications of the Department of Homeland Security [DHS], reports of several commissions and committees to assess the functioning of homeland security periodically), as well as secondary literature on risk and risk management as a security practice.

The concept of homeland security emerged in the US before 9/11, but was officially adopted as a policy immediately after the attacks and the declaration of the global war on terror (GWoT). Subsequently, the DHS was created as an umbrella organisation through a massive overhaul of the existing security apparatus in the US. Homeland security subsequently has been undergoing constant expansion in its meaning and definitions, moving from a predominantly terrorism focus

* Assistant Professor, Department of Political Science, Bharati College, University of Delhi, New Delhi. Email: shailza134@gmail.com

to an all-hazards approach. Though largely concerned with domestic security, it involves a unique perception of the international strategic landscape, giving rise to newer ways of assessment of threat as well as addressing them. The threat assessment is based on the efforts to gain knowledge about the risks from unpredictable, uncertain and chaotic sources in the international area. The governance framework of homeland security is based on risk assessment and risk management that rests on highly advanced technology and computerised data mining. Information technology is leveraged to come up with 'smart' policy solutions. The framework is also spreading globally through overseas missions and bilateral dialogues with countries of Europe, Asia and Africa. This US model of homeland security is on its way to becoming a global model.

It is argued in this paper that addressing security through a risk framework supported by a proactive overhaul of existing understanding and practices aims at generation of a new knowledge structure about how security is perceived in contemporary times across the globe. It is further argued that such a perception about security is instrumental in generating an embedded sense of pervasive insecurity, as security ceases to be characterised by absence of fear. Rather, it becomes a function of everyday minimisation of risk situations. While the latter becomes a self-perpetuating exercise, the threat perception based on 'riskiness' indicated through the risk levels from a range of identified sources (from terrorism to natural hazards to pandemic diseases: all having the potential to spread with an alarming rate and reach) becomes a constant.

The paper attempts to address the following research questions: How has risk become a keyword around which security governance is being organised? How is it reflected in security praxis? What kind of debates has risk management generated in security studies? Finally, how do these debates contribute to an understanding of the nature of security in the contemporary world? The paper is divided into four sections. The first section deals with the origins of the concept of risk as a subject of enquiry in the social sciences and its linkage with governance. The second section explores security governance as risk management with reference to an analysis of US homeland security. This section also situates homeland security analysis in the context of debates in international security studies on risk and risk management. The final section explores the

linkages between risk management practices, technology and security. This section is followed by a conclusion.

I. Risk as a Defining Feature of the Modern World

Risk as a characteristic and outcome of modernity came up as a matter of reflection as early as the 1990s in the works of sociologists Ulrich Beck and Anthony Giddens. In 1992, Ulrich Beck developed the idea of transition of the modern industrial society into a risk society. Talking as a reflexive modernist, he argued that technological advance in modern society has given rise to a range of uncertainties encompassing most aspects of human existence. These risks are the creation of modernity and are different from those that existed in the past. They are instrumental in causing irreversible damage and are also not restricted to any one country (Beck 1999). However, he later modified his argument and put forth the idea of *world risk society*. He highlighted the feature of world society where not just the existing risks, but the anticipation of possibilities of risks in future, become the basis for response measures. Thus, risks assume the attribute of perpetuity, calling for continuous anticipation and prevention, having no end. Still later he coined the term 'manufactured uncertainties' for risks as an unavoidable human creation and not something external to society. Explaining the sociological category of risk he says that '(risk) consumes and transforms everything… is like the acid bath in which venerable classical differences are dissolved…is not a catastrophe but the anticipation of future catastrophe in the present…is existent and non-existent, present and absent, doubtful and real…it can be assumed to be ubiquitous and thus grounds a politics of fear and a politics of prevention' (Beck 2009: 3).

Beck thus attributes risk with features that get superimposed on the basic characteristics of anything that it gets associated with, leading to the fading away of the prior identity. This enables interventions of an extraordinary nature. For example, a risky group or individual or territory or phenomenon necessarily demands corrective treatment in the present, whether or not its potential to cause damage in future is factually established. In such a scenario, how risks get defined is something that needs to be a serious concern.

The beginning of the 21st century has been characterised by the application of risk-based approaches to governance across policy areas. The precepts of such approaches rest on the idea of 'vulnerability', which in turn informs risk assessment. A report by the UNDP includes a Disaster Risk Index (DRI), where risk is measured in terms of the number of deaths during disasters. It defines 'human vulnerability' as a human condition process resulting from physical, social, economic and environmental factors, which determine the likelihood and scale of damage from the impact of a given hazard. The term 'human vulnerability' refers to the different variables that make people more or less able to absorb the impact and recover from a hazard event (UNDP 2004: 98).

A range of scholarship highlights how governance is reorganised through 'risk'-based understanding (Demerrit 2014; Krieger 2013; Rothstein 2013). These studies problematise different aspects of the linkage between risk and governance. For instance, Demeritt describes the concept as having connotations for creating a certain way of understanding. 'Risk, in this sense, is not a real thing-in-itself but an epistemological descriptor'. He further argues that risk cannot be definitively forecasted and is also indeterminate (Demeritt 2014).

Defining the Threat Environment: Security through Risk Management

The 9/11 terrorist attacks came from non-state actors whose location was not immediately traceable, hence unknown. Also, since terrorism came to establish itself as transnational network-based organised crime, the source of threat came to be understood as globally dispersed. Thus, the threat and the probability of its occurrence were transported to the realm of the 'unknown'. What was inferred in terms of the threat situation was the catastrophic nature of the threat, the responsibility of the state authority to asses and manage the uncertain and the uncontrollable.

The threat environment thus came to be defined through the concept of risk. This concept entails the existence of a diversity of sources which are capable of causing catastrophic damage, are uncontrollable, defy attainment of complete security at any point in time, and therefore cannot be handled with the existing mechanisms of guaranteeing security. Consequently, the need for a

departure from past understandings was highlighted and the case for newer ways of risk assessment and risk management was made. It is important to note here that the US has been the main propeller of these developments as the 9/11 terrorist attacks took place on its territory.

However, in the aftermath of the attacks, the onus for tackling the terrorist menace was framed as a global responsibility, as evident from the subsequent launch of the 'global' war on terrorism. Consequently, an equally important development was the cultivation and propagation of a homogenous set of guidelines in the form of policy framework. This framework is supposed to inform the security policies adopted in different countries. The homeland security paradigm (the policy framework with all its constitutive elements including the ideas, the mission and technologies) originated in, but is not confined to, the US alone. It is promoted and propagated through bilateral partnership dialogues with other countries. Also, there are international platforms for consolidating homeland security as an international regime.[1]

II. Homeland Security and Risk Management

Today, governments are increasingly employing a language that communicates the gravity of a threat environment in terms of uncertainties which are qualitatively different from the ones that existed in the past. Here, the case of homeland security in the United States is discussed to explore the nature of intervention of a risk-based approach in security and the understanding/s it has produced in security studies.

In a risk-based approach to security, threat is perceived from a whole range of sources, from terrorism to cyberspace to natural disasters, pandemic diseases leading to a 'riskisation' of a threat environment. The term homeland security became official vocabulary in the United States after the terrorist attacks of September 11, 2001. Immediately after the attacks, the Office of Homeland Security was created with the objective of having an institutionalised response mechanism to the terrorist threat. Later, in 2002, a full-fledged Department of Homeland Security came into existence with the objective of preventing the American homeland from terrorist attacks. In the subsequent years, the Department adopted an all-hazards approach, that

is, from a terrorism focused approach to a 'homeland security enterprise' that would include threat assessment from other catastrophic events like natural disasters and pandemic diseases.

However, the effective utilisation of the grants made under the head of homeland security was something that invited criticism from a number of sources like the state and local leaders. This was taken cognisance of by the 9/11 Commission which mentioned in its report that: 'Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities'[2] (The 9/11 Commission Report 2004: 396).

In the confirmation hearings before the Committee on Homeland Security in the House of Representatives in 2005, the then Secretary of Homeland Security, Michael Chertoff, emphasised that the 'DHS must base its work on priorities driven by risk'. He also mentioned that the department's efforts are based on risk assessment and mitigation, though it lacks the expertise that the financial and insurance industries have in this area.[3]

Subsequently, several steps were taken to ensure that the risk-based approach to homeland security is consolidated. The 2007 National Strategy for Homeland Security (NSHS) reiterated, in categorical terms, the significance of risk management to the functioning of the department mentioning that

> The assessment and management of risk underlies the full spectrum of our homeland security activities, including decisions about when, where, and how to invest in resources that eliminate, control, or mitigate risks…we accept that risk—a function of threats, vulnerabilities, and consequences—is a permanent condition. We must apply a risk-based framework across all homeland security efforts….A disciplined approach to managing risk will help to achieve overall effectiveness and efficiency in securing the Homeland. In order to develop this discipline, we as a Nation must organize and help mature the profession of risk management by adopting common risk analysis principles and standards, as well as a professional lexicon (DHS 2007: 41).

Subsequently, the DHS Office of Risk Management and Analysis was created in 2007 as part of the National Protection and Programs Directorate with the objective of generating rigorous and

systematic risk analysis methodologies and technological capabilities to assess and measure risk. Also, the emphasis was on developing a uniform methodology and guidelines to avoid ambiguities and facilitate smooth funding. The DHS Risk Steering Committee (RSC) was created to provide nationwide uniform guidelines for the governance of homeland security that same year. The mandate of the Committee was to provide a comprehensive taxonomy of risk-related terms and their meanings, crucial for the functioning of homeland security risk assessment and management. The first document to this end, entitled *DHS Risk Lexicon*, was published in September 2008 and the next one in 2010. It generated a list of 73 terms and their meanings that were seen to be of crucial significance to the practice of homeland security. The Committee has frequently generated guideline documents and also seeks to foster national and internal partnerships.

The 2010 *Quadrennial Homeland Security Review* Report also reiterated the centrality of effective risk management as the fundamental task of homeland security (DHS 2010). Further, the DHS produced a Homeland Security Risk Management Doctrine entitled *Risk Management Fundamentals* in April 2011 with the objective of consolidating the department's role in 'leading the unified effort to manage risks to the nation from a diverse and complex set of hazards, including acts of terrorism, natural and manmade disasters, pandemics, cyber attacks, and transnational crime' (DHS 2011: 7).

The risk lexicon generated a taxonomy that constitutes a comprehensive doctrine of homeland security risk management. The doctrine highlighted that the 'dynamic' and 'uncertain' nature of the world makes it too complex to be handled according to the ways of the past. The probability of all these as potential sources that can cause damage is expressed through the term 'risk', where risk is defined as 'the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences' (DHS 2010: 27). The risk scenario is expressed as one that can have 'large and unanticipated cascading effects throughout American security' (DHS 2011:7) Thus, guaranteeing security is made contingent upon risk assessment and risk management, where the latter has been defined as: Risk management is the process for identifying, analyzing, and communicating risk and accepting,

avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken' (DHS 2010: 30) Also, homeland security requires a proactive effort to popularise this framework across all levels—local, national and international.[4]

III. The Transformation of Security to Risk Management: Interpretations in International Security Studies

The idea behind the set of exercises pertaining to homeland security is to address the concerns of security through a 'risk framework' by generating common understanding about how the threats need to be understood in contemporary times, as well as about the mechanisms through which they should be addressed. The Lexicon defines threat as: 'a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property' (DHS 2010: 36). The threat spectrum is generated through calculating what all is likely to pose a danger in future and is reflected through the coinage, 'vulnerability'. The Lexicon defines vulnerability as 'physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard' (ibid.: 38). This amounts to not just preparedness to real threats, but also to creating a way of thinking about how threats need to be thought of.

This discussion demonstrates that the war on terror infused the risk vocabulary to the domain of security. Risk management has come to be the modus operandi of security practices. Scholars of international security studies argued as early as 2001 that risk has come to be the defining feature of the threat environment of the post-Cold War period, and risk management has become the main task of security governance.

Ole Waever's securitization theory argues that issues are handled as security problems to strengthen governmental control and limit the possibilities of political debate and discussion.[5] He hints at the transformed nature of the handling of security issues. Hans Gunter Brauch, in his analysis of the concepts of threats, risk and vulnerabilities, mentions the argument of Ole Wæver that today's considerations of safety are increasingly about managing risks rather than achieving perfect security (Ole Waever cited in Brauch 2011: 85).

Several studies argue that governing through risk assessment is an exercise in disciplining the reality (present as well as the future) in a particular manner, putting in place controls that mould everyday practices and providing them a rationale that normalises the exceptional (Bigo 2002; Werner 2005, cited in Ardau and Munster 2007).

Oliver Kessler classifies the current scholarship on risk in security studies into three categories (Kessler 2010). The first category comprises Ulrich Beck's risk society proposition, which was revised as world risk society after 9/11. It highlights the global and uncontrollable nature of threats with emphasis on the aspect of uncertainty associated with them. The uncertainty creates 'regimes of non-knowledge' and consequent inability to calculate. This, however, does not absolve the states of their responsibility to address the threats. Risks thus embody the efforts of the states to address the non-knowable and uncontrollable by imposing an ontology through definition, thus involving a power relationship. This is done by adopting precautionary or preventive measures to appear to be in command when actually they are not (ibid.: 18,19).

The second category belongs to the tradition of Focauldian scholarship which posits risk as the new *dispositif*[6] of security politics. This is represented by the works of Claudia Ardau and Rens van Munster. This body of work highlights the constructed nature of risks and the politics that such a construction is part of to justify certain practices as rational. The uncertainty is converted into risk to 'impute' rationality where it doesn't apply. They highlight as example the politics and lobbying efforts of industries that led to the passage of TRIA (Terrorism Risk Insurance Act) in the US (ibid.: 20). The third category of scholarship represented by the work of Niklas Luhmann looks at risk as a way of ascribing meanings in a manner that alters the relationship between the social, economic and political. Hence, it highlights the absence of any objective risk. Risk acquires meaning only in relation to the concepts that it is related with to arrive at a meaning (ibid, 21, 22).

Analysing all these strands, Kessler argues that there is no single approach to risk in security studies; rather, there are multiple interventions attempting to interpret the shift to a risk

framework in security studies. However, the thread running through all these interventions indicates that risk thrives on uncertainty. This uncertainty is qualitatively different from the uncertainty that traditional security studies signified.

Hence, the understanding of security through risk marks a 'systemic shift'. It is not just a shift from the state to the private and transnational actors, it also marks a shift from positivist rationality. This is not genuine uncertainty; rather, the interplay between uncertainty and risk gives rise to further production of uncertainty, or what is expressed as *redefined production of social contingency*. Uncertainty then becomes a function of technologies of risk management leading to commodification of security. This is 'a necessary shift in the knowledge structure of world politics', and a departure from the past ways of knowledge and understanding (Kessler 2010: 24, 25).

IV. Technology, Risk and Security

The transformation of security into risk management is not imaginable without the crucial component of technology. It is thus demonstrable that this transformation rests on the conditions created by technological sophistication. While Beck highlighted the role of technology in the advent of risk society, the foregoing discussion highlights the fact that much of the process of conversion of uncertainties into risk through identification of vulnerabilities as well as the process of risk management itself rests on technological sophistication.

On the one hand, the risk from non-knowledge of the source of threat cited as technology-driven, while on the other hand the assessment and response also rests on precautionary technological intervention. However, this should not be read as a neutral, technology driven involuntary process, but rather, it is inherently political in terms of who gets to define what constitutes a risk as well as the timing and nature of intervention. The homeland security enterprise today defines the 'risk' of terrorism for the entire globe and also provides the policy prescriptions to all nations, big and small. The policy prescriptions rest on the risk analysis methods and modelling based on huge data sets. The items included in the 'risks basket' have been constantly increasing since then, incorporating within its fold natural disasters, pandemics,

economic downturns, as mentioned before. While this amounts to universalisation and standardisation techniques in areas that require a variegated intervention and response mechanism, it also hints at the power dimension that the risk-based framework embodies.

Former US Homeland Security Secretary Tom Ridge (2002) observed that 'Terrorists can sit at one computer connected to one network and can create world havoc… [they] don't necessarily need bombs or explosives to cripple a sector of the economy, or shutdown a power grid'. While describing the risk from terrorism, the risks to the economy and the power sector are also incorporated, thus giving rise to what Kessler calls *redefined production of social contingency* (discussed in the previous section). He outlines the processing of uncertainty as such: 'Uncertainty is always reduced to risk by social systems (i.e. by processes of categorization, world disclosure, interpretation and observation, etc.) thereby producing new internal contingencies and uncertainties in the form of other excluded alternatives, other possible worlds and perspectives that always makes one's own position contingent and fluid' (Kessler 2010: 22). Hence the subsequent redefining of the homeland security mission from a terrorism-centric to an all-hazards approach.

There is also evidence of how the precautionary or preventive regimes are slipped through, deriving their legitimacy from the risks framework aided by technologies of risk management. The global war on terror created a regime of 'pre-emption', i.e., to prevent the attacks before they occur. This pre-emption rests on risk assessment.

There are several studies that look at the politico–technological aspect of such precautionary risk assessment and management. A recent study discusses how the 'war on terror' has given rise to new politically significant techniques of imagining the future. Richard Grusin, building on the media theory of *remiadtion,*[7] terms this phenomenon 'premediation', that 'works to prevent citizens of the global mediasphere from experiencing again the kind of systemic or traumatic shock produced by the events of 9/11 by perpetuating an almost constant, low level of fear or anxiety about another terrorist attack' (Grusin 2010: 2).

The 2002 National Homeland Security Strategy emphasised the concept of creating 'Smart Borders' of the future, using advanced technology to track the movement of cargo and the entry and exit of individuals (White House 2002). This resulted in the launch of the US-VISIT (United States Visitor and Immigrant Indicator Technology) programme—an automated entry–exit tracking system. It came up as a US$ 10 billion project with the objective to structure immigration systems of all sea, land and air ports of entry, employing the techniques of risk management. It requires prescreening of all US-bound travellers, classifying them as low-risk or high-risk traffic. These practices are instrumental not only in creating newer ways of border control for governing mobility, but also newer understandings about the borders themselves.

Drawing on the US-VISIT border programme, one study introduces the term *biometric borders* to communicate the practice of border management based on digital technology and data integration managerial expertise. It is argued that the concept of 'smart border' finds completion in the idea of 'virtual borders'. The concept of smart border seeks to govern mobility and regulate different aspects of daily life, thus securitizing day-to-day living through technological sophistication (Amoore 2006: 338). Border management thus tends to become biopolitical from being a matter of geopolitical policing, and the border becomes a 'virtual' site through which the behaviours and daily practices of populations can be made amenable to intervention and management (Amoore and Goede 2005: 160). Benjamin J. Muller coined the term 'biometric state'[8] to explain such governing through risk by employing a range of technologies of risk management, emphasising the role of imagination in the entire exercise (Muller 2010).

Information warfare, information operations, information assurance, cyber-terrorism and similar words have become common vocabulary in official policy documents and security doctrines of the present times. The website of the Department of Homeland Security mentions that the DHS Science & Technology Office of Public-Private Partnerships (P3) engages industry and facilitates partnerships with private sector innovators to advance commercial technology solutions that address homeland security challenges.[9] Firms like Risk Management Solutions (RMS), a catastrophe risk modelling company, provide policy advice through mathematical risk assessment modelling to understand, quantify and manage risk from earthquakes, hurricanes,

floods to terrorism and infectious diseases. These provide governments significant tools in risk management policies. The US Department of Homeland Security entered into a contract with management consultants Accenture in 2005, aiming to make it fully functional within a decade to assist the Department's border management efforts (cited in Amoore 2006).

The technology-centred aspect of risk management in the war on terror highlights the role of big companies that provide the technological expertise, management consultation, as well as the sophisticated equipment for screening, surveillance, etc. Homeland security equipment exhibitions and management workshops are now a regular feature, not only in the US, but also in several other countries where homeland security bilateral cooperation agreements have been put in place.

This aspect of risk management has invited response in security studies. It is argued that 'the management of risk is big business. Risk points to a transnationally organized discourse, shaped by a multitude of rationalities including insurance companies, banks, hedge funds, private business' (Ardau and van Munster 2007 and Peterson quoted in Kessler 2010: 24). Further, it is also said that 'as such, security becomes increasingly a question of the right technical solutions, and not a question of justice or social and political reform' (Kessler 2010: 24).

Amoore and Goede cite the work of criminologists Mariana Valverde and Michael Mopas to describe risk management policies as a shift of focus from the ability to produce a risk-free society to 'targeted governance' defined as a 'limited risk-driven intervention into society based upon a dream of a smart, specific side-effects free information driven utopia of governance' (Amoore and Goede 2005: 150). The study also highlights *dataveillance*, an important aspect of this targeted governance and its risk assessment. Dataveillance is defined as proactive surveillance of what become effectively suspect populations, using new technologies to identify 'risky groups' (Roger Clarke, David Wall and Mike Levi, quoted in Amoore and Goede 2005: 151).

It is argued that 'risk management should be considered as a regulating form of security that permanently identifies, classifies and constitutes groups and populations on the basis of risk

ascribed to these groups' (van Munster 2005: 6). Risk management deals with potential rather than existential threats. It does not operate on the basis of stable identities and is preventive in nature. It transforms security from the 'exceptional decision outside the normal' to something that increasingly permeates everyday life. Risk management gives rise to large scale surveillance societies infested with feelings of fear, anxiety and unease (van Munster 2005). This kind of risk assessment strategy is employed heavily in the counter-terrorism policies of the war on terror. There are numerous studies, news reports and even movies on how religion and regions have been the basis of presumptively profiling people and places as risky or dangerous.

The risk analysis methods prescribed as the need of the hour are ridden with serious limitations. A review of the Department of Homeland Security's Approach to Risk Analysis highlights the statistical limitations to the assessment of terrorism related risk through the risk-analysis methods and enumerating the challenges to risk analysis for homeland security (NRC 2010). This highlights the politics of risk management more than the adequacy of risk management as a policy solution to security problems of contemporary times.

V. Conclusions

Threats are predominantly defined through the language of risks in contemporary times. The global war on terror spurred a momentum where gradually not just terrorism, but threats from a diversity of sources, came to be assessed in terms of risk. While security for states has been largely about calculations in the context of uncertainty, the nature of uncertainty that the risk framework thrives on is qualitatively different. Looking at the case of homeland security in the US, it is observed that the heavy reliance on technology-based imaginative modelling presumes a departure from past threat assessment. The processing of uncertainties into risks has led to pre-emptive policy regimes implemented as risk management. The emphasis on the non-knowledge of the source of threat and the uncontrollable nature of both the threat as well as the consequence is captured through the expression of vulnerability. This indicates that the risk framework attempts to alter the knowledge structure of security by providing a new set of tools to arrive at the meaning of security. This alteration is mediated by the state in alliance with high-end technology asserting their power to govern in this process. The transformational vocabulary

employed by the government for threat assessment is used to justify the heavy reliance on technology for risk management. This hints at the political economy of the technology industry consolidating through a neo-liberal, security-market model in our times as assurances of risk minimisation rest on huge budgetary allocations.

However, what needs intensive research is the impact of such policies in generating a sense of security in society. There are many levels of friction. The 'preemptive fixing of identities' that the concept of biometric borders seeks to fully employ has already been taken up as a cause of concern by many immigrant rights groups, civil liberties and privacy organisations, and other civil society advocacy groups. Critics argue that in the name of more security for citizens, the state is 'terrorising the society'. These newer technologies and methods tend to make citizens more fearful and protective rather than secure.

Notes

[1] The US–India Homeland Security Dialogue was launched in May 2011, and the US–Africa one in 2016, focusing on homeland security and counter-terrorism cooperation. These dialogues seek to extend the US's understanding of the 'Homeland Security Enterprise' to other countries, aiming to pave the way for specialised training programmes and gradually building an army of experts who can handle new technologies and mechanisms to deal with various kinds of terrorism and anti-national activities. There is also an international organisation called the Global Society of Homeland and National Security Professionals.

[2] The National Commission on Terrorist Attacks upon the United States, also known as the 9-11 Commission, was created as an independent, bipartisan commission by congressional legislation and the signature of President George W. Bush in late 2002. The Commission's mandate was to prepare a full and complete account of the circumstances surrounding the September 11, 2001 terrorist attacks, including preparedness for and the immediate response to the attacks. The report of the commission was released in July 2004 and can be accessed online at https://www.9-11commission.gov/report/911Report.pdf

[3] The Secretary's Second-Stage Review: Rethinking the Department of Homeland Security's Organisation and Policy, Part 1 and 2. Hearing before the Committee on Homeland Security 109th Congress. Serial No. 109 -32. p7. Accessed on May 20, 2018.url: https://books.google.co.in/books?id=CU_lIHsTfEC&pg=PA7&lpg=PA7&dq=DHS+must+base+its+work+on+priorities+driven+by+risk&source=bl&ots=dOSIyuluFp&sig=v15zOBxcJz6PSVtSPGEr8LIEiXM&hl=en&sa=X&ved=0ahUKEwjAp9L26_XbAhWJfH0KHTElAeoQ6AEIJjAA#v=onepage&q=DHS%20must%20base%20its%20work%20on%20priorities%20driven%20by%20risk&f=false

[4] The 2002 National Strategy for Homeland Security (NSHS) defined homeland security as a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimise the damage and recover from attacks that do occur (DHS 2002: 2). Further, it outlines that its objectives constitute an exceedingly complex mission. It involves efforts both at home and abroad. It demands a range of government and private sector capabilities. And it calls for coordinated and focused effort from many actors who are not otherwise required to work together, and for whom security is not always a primary mission (ibid.: 3)

[5] Securitization theory is associated with Ole Waever in international relations. Its main argument is that security is a social and inter-subjective construction. By stating that a particular referent object is threatened in its existence, a securitizing actor claims a right to extraordinary measures to ensure the referent object's survival. The issue is then moved out of the sphere of normal politics into the realm of emergency politics. Securitization means bringing an issue into the security realm and treating it as a security matter (Waever 1998).
[6] Michel Foucualt defined his usage of the term *dispositif* in 1977 as 'a thoroughly heterogenous ensemble consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions. The *dispositif* is the system of relations that can be established between these elements.' https://foucaultblog.wordpress.com/2007/04/01/what-is-the-dispositif/
[7] The theory of mediation developed by Grusin and Jay Hold talks about the logical opposition between reality and mediation, i.e., reality as it comes to appear through the intervention of media. The concept of premediation connotes the media logic that emerged after the September 11 attacks as a form of 'medial pre-emption'.
[8] Muller says that a biometric state is the consequence of the contemporary obsession with technologies of risk and praxis of risk management. The biometric state is characterised by the prevalence of virtual borders and is based on biometric identifiers such as passports, trusted-traveller programmes and national ID cards, as well as the associated forms of social profiling.
[9] Visit https://www.dhs.gov/science-and-technology/office-public-private-partnerships.

References:

Amoore, L. and Marieke D. Goede. 2005. 'Governance, Risk and Dataveillance in the War on Terror', *Crime, Law & Social Change,* 43: 149–73. Accessed on 12 April 2018. url: http://community.dur.ac.uk/contested.borders/wp-content/uploads/2016/02/Governance-Risk-and-Dataveillance-in-the-War-on-Terror.pdf

Amoore, Louise. 2006. 'Biometric Borders: Governing Mobilities in the War on Terror', *Political Geography,* 25: 336–51. Accessed on 12 April 2018. url: http://www.antoniocasella.eu/nume/Amoore_2006.pdf

Aradau, Claudia and Munster, Van Rens. 2007. 'Governing Terrorism Through Risk: Taking Precautions, (un)knowing the Future'. European Journal of International Relations. Vol. 13, Issue 1, pp. 89-115.

Beck, Ulrich. 1999. *World Risk Society*. Cambridge: Polity Press.

———— 2009. 'World Risk Society and Manufactured Uncertainties', *IRIS European Journal of Philosophy and Public Debate*, October: 291–99.

Bigo, D. 2002. 'Security and Immigration: Towards a Governmentality of Unease', *Alternatives/Cultures & Conflicts,* Special Issue: 63–92.

Brauch, H.G. 2011. 'Concepts of Threats, Challenges, Vulnerabilities and Risks', in H.G. Brauch et al., *Coping with Global Environmental Change, Disasters and Security: Threats, Challenges, Vulnerabilities and Risks*, pp. 61–106. Springer.. Accessed on 25 June 2018. url: ps://www.researchgate.net/publication/299757745_Concepts_of_Security_Threats_Challenges_Vulnerabilities_and_Risks.

De Goede, Marieke. 2008. 'Beyond Risk: Premediation and the Post-9/11 Security Imagination', *Security Dialogue*, 39: 155–76

Demeritt, David. 2014. 'Risk Governance: From Governing Risk to Governing Through Risk'. Accessed on 15 May 2018. url: https://www.researchgate.net/profile/David_Demeritt/publication/270157362_Risk_Governance_From_Governing_Risk_to_Governing_Through_Risk/links/54a128670cf267bdb9018040/Risk-Governance-From-Governing-Risk-to-Governing-Through-Risk.pdf

DHS (US Department of Homeland Security). 2007. *National Strategy for Homeland Security*. Washington D.C. Accessed on 20 January 2018. url: www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

————— 2008. *Strategic Plan for Fiscal Years 2008–13. One Team, One Mission, Securing Our Homeland*. Washington D.C. Accessed on 20 January 2018. url: https://www.fdle.state.fl.us/Content/getdoc/67e98737-3bf6-4cff-bda1-78ee2061b2c3/DHSStrategicPlan2008-2013.aspx

————— 2010a. Quadrennial Homeland Security Review (QHSR) Report. *A Strategic Framework for Secure Homeland*. Washington D.C. Accessed on 15 March 2018. url: https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

————— 2010b. Risk Steering Committee. *DHS Risk Lexicon*. Washington D.C. Accessed on 15 March 2018. url: https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

————— 2011. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine.* Washington D.C. Accessed on 15 March 2018. url: https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf

Grusin, R. 2010. *Premediation: Affect and Mediality After 9/11*. UK: Palgrave Macmillan.

Kessler, Oliver. 2010. 'Risk, in J. Peter Burgess (ed.), *Routledge Handbook of New Security Studies*, pp. 17–26. Oxon: Routledge.

Krieger, K. 2013. 'The Limits and Variety of Risk-based Governance: The Case of Flood Management in Germany and England', *Regulation and Governance*. doi: 10.1111/rego.12009.

Muller, Benjamin J. 2010. *Security, Risk and Biometric State: Governing Borders and Bodies*. New York: Routledge.

Munster, van Rens. 2005. 'The EU and the Management of Immigration Risk in the Area of Freedom, Security and Justice.' Political Science Publications: University of Southern Denmark.

NRC (National Research Council of the National Academies). 2010. Review of the Department of Homeland Security's Approach to RISK ANALYSIS: Report of the Committee to Review the Department of Homeland Security's Approach to Risk Analysis. Washington D.C.: The National Academies Press.

Rothstein, H. 2013. 'Exploring National Cultures of Risk Governance'. Accessed on 14 June 2018. url: http://www.lse.ac.uk/accounting/Assets/CARR/documents/R-R/2013-Spring/CARRmagRR25-Rothstein.pdf

The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States. 2004. Authorized Edition. New York: WW Norton and Company. Accessed on 1 June 2018. url: https://www.9-11commission.gov/report/911Report.pdf

UNDP, Bureau for Crisis Prevention and Recovery. 2004. *A Global Report: Reducing Disaster Risk A Challenge for Development.* New York.

White House, US US Office of Homeland Security. 2002. *National Strategy for Homeland Security*. White House: Washington D.C. 16 July. Accessed on 20 January 2018. url: http://www.whitehouse.gov/homeland/book/index.html

Wæver, Ole. 1998. 'Securitization and Desecuritization', in Ronnie D. Lipschutz (ed.), *On Security*, pp. 46–87. New York: Columbia University Press.