Developing a systems failure model for aviation security

Author:

Paul McFarlane, PhD

Department of Security and Crime Science
University College London
35 Tavistock Square
London
WC1H 9EZ

Email: p.mcfarlane@ucl.ac.uk

Abstract:

This paper presents an entirely new perspective to explain aviation security failure. Aviation security failure is conceptualised by analysing the official report by the National Commission on Terrorist Attacks Upon the United. The National Commission report is an authoritative and data-rich account of aviation security failure that, hitherto has never been made available for scientific research. The results introduce new concepts such as erroneous perception, system cognition and desensitisation, and the data are used to propose a new systems failure model for aviation security. The paper concludes by suggesting aviation security, by its unique construction, can be predisposed to failure.

Keywords:

Aviation security
System failure
Aviation terrorism
Complex systems

Highlights:

- Lack of conceptual analysis of aviation security failures
- Aviation security is predisposed to failure
- Aviation security is a complex system
- Interactions between system elements are complex and difficult to predict

1. Introduction

On the 11th September 2001 (henceforth 9/11), the aviation security system in the United States—unexpectedly—failed even though it was "blinking red", warning of impending collapse (The National Commission on Terrorist Attacks upon the United States, 2004a). It failed in its objective to facilitate the free flow of passengers and goods and provide resistance to direct attack by terrorists or other threat groups. In overcoming the security layers, the terrorists revealed numerous modes of system failure. These 'modes of failure', created by the combination of a unique set of fortuitous circumstances, had been present in the system for many years.

Mitigating the risk of routine operation airports has been the focus of significant academic research (see Iervolino et al., 2019). In similar security systems, modes of failure, can be attributed to high-level (human) decision-making processes that design, operate and manage these types of systems (Reason, 1990; 2008).[1] In terms of why these systems do not respond to warnings and unexpectedly fail, the related literature identifies a dislocation between two important theoretical positions. Firstly, the notion that system failures are an unavoidable and inevitable consequence of the complex interactions between system elements (Perrow, 1999). Secondly, failures are preventable if the system recognises the warnings signs in advance and takes mitigating action (Turner, 1976; Toft and Reynolds, 2005). Also, the literature, rather than exploring causation of failure, is dominated by studies which argue for using more complex security technologies (International Civil Aviation Organisation, 2011; Riley, 2011) to bridge identified gaps in the system.

Technological reliance increases complexity and risk. These studies alone are therefore insufficient to understand the problem of aviation security failure. To mitigate future risk, aviation security needs to move beyond being reactive and backwards-looking (Jenkins, 2012; La Tourrette and Jenkins, 2012)—towards a smarter system cognisant of the recurrent risk of failure. However, there has not yet been a detailed conceptual analysis which considers the features of the recurrent risk (Jenkins, 2012). Therefore, the aim of this paper is to present an entirely new perspective to the evolving theoretical discourse around aviation security failure. The paper recommends a new systems failure model for aviation security and offers academics

[1] These were human-mediated modes of failure, i.e., vulnerabilities in system defences that are consequential to how human operators interact with other elements, organisational structures and processes in the wider system.

and practitioners an original way of conceptualising the risk of failure of such a critical system. The paper concludes by proposing that aviation security, by its unique construction, can be predisposed to failure.

2. Methods

2.1 Research design

This study used a qualitative research design. It was broadly Interpretivist and used the single-case study method to thematically analyse the content of the official report by the National Commission to explore the security system failure on, and before 9/11. The rationale for selecting this design was twofold. Firstly, case-study approaches have been successfully used by many researchers to analyse large-scale systems failures (see Aini and Fakhrul-Razi, 2010; Perrow, 1999; Turner, 1976, 1978; Turner and Pidgeon, 1997; Toft and Reynolds, 1999). Secondly, it offered a unique opportunity to "observe and analyse a phenomenon previously inaccessible to social science inquiry" (Yin, 2009). Although, not the case for this study, a potential weakness of the single-case design is that the nominated case (after initial exploration) may not be the case that it was thought to be at the time of selection (Yin, 2009). Also, the researcher adopted a self-reflective approach and, sought as far as possible in this case, to act with objectivity and detachment.

2.2 Data collection and analysis

Thematically analysing (socially constructed) documents from the process of inquiry of witnesses, is a widely used qualitative research method (Gilbert, 2008). In this case, the National Commission report remains a most authoritative and data-rich account of aviation security failure. It can itself be described as a thematic analysis of more than 2.5 million pages of documents and interviews of the real-world experiences of over 1200 persons (National Commission on Terrorist Attacks upon the United States, 2004b). While the report is for reasons other than scientific research, it is—without dispute—a document which is "socially produced" (McDonald, 2001). It can, therefore, be used to provide unique insights into the perceived realities and experiences of those involved in the security system at that time.

As a single-case, thematic content analysis (TCA) was used to study the National Commission report. TCA is an analytic method frequently used in qualitative research to recognise patterns and describe phenomena (Boyatzis, 1998; Braun and Clarke, 2006; Fereday and Muir-Cochrane, 2006; Roulston, 2001). A recognised variant of TCA is template analysis. Template analysis (TA) was used to organise the data according to a set of a-priori themes. TA, a derivative of more formal methods, is not directly tied to realist methodologies (Waring and Wainright, 2008). Therefore, it allowed the researcher to consider the data deductively while at the same time providing space for the inductive emergence of new themes and concepts (Crabtree and Miller, 1999).

The template and codes were deductively developed by following the guidance provided by Boyatzis (1998). The codes related to themes from Turner's (1976) human-made disasters; Reason's (1990) generic error modelling system and organisational accident model; Weigman and Shappell's (1997) Human Factors Analysis and Classification System; Toft and Reynold's (2005) systems failure and cultural readjustment model. Some codes were revised after testing against the executive summary and a selection of key statements in the official report.

The template was applied to systematically review 567 pages of data within the National Commission report. The researcher, using NVivo, coded relevant segments of data using the deductive theory-driven codes in the template. Further codes and themes were also identified inductively and recorded using NVivo. On completing the coding, these data were sorted into a broader group of themes. Then, through a process of iteration, the overarching theme (Braun and Clarke, 2006) of 'predisposition to failure' was developed to provide a conceptually driven explanation of the phenomena.

3. Results

The results can be summarised by saying the system was constructed in a way where it was predisposed to exploitation and failure. Table 1 presents the main and subsidiary themes and Figure 1 outlines the linkages between each theme.[2] This notion is relevant in two ways. Firstly, to pronounce the consequence of the conditions that were found to exist within the system during the analysis. Secondly, to argue that, more generally, in such a real-world social system, the inherent flaws relating to human imperfection could negate the possibility of ever constructing an infallible system. The emergent themes are closely associated, in one way or another, with the managing, processing and comprehension of information that flows throughout the layers and elements of the system.

[2] Appendix A provides a selection of extracts from the dataset for each of the identified themes.

Predisposition to failure
1: Erroneous perception of threat
2: System alignment
3: System inertia
4: Blocked information pathways
5: Desensitization towards opportunities
6: Towards a critical condition
7: Imagination
8: Failure to respond to warnings

Table 1: Main and subsidiary themes

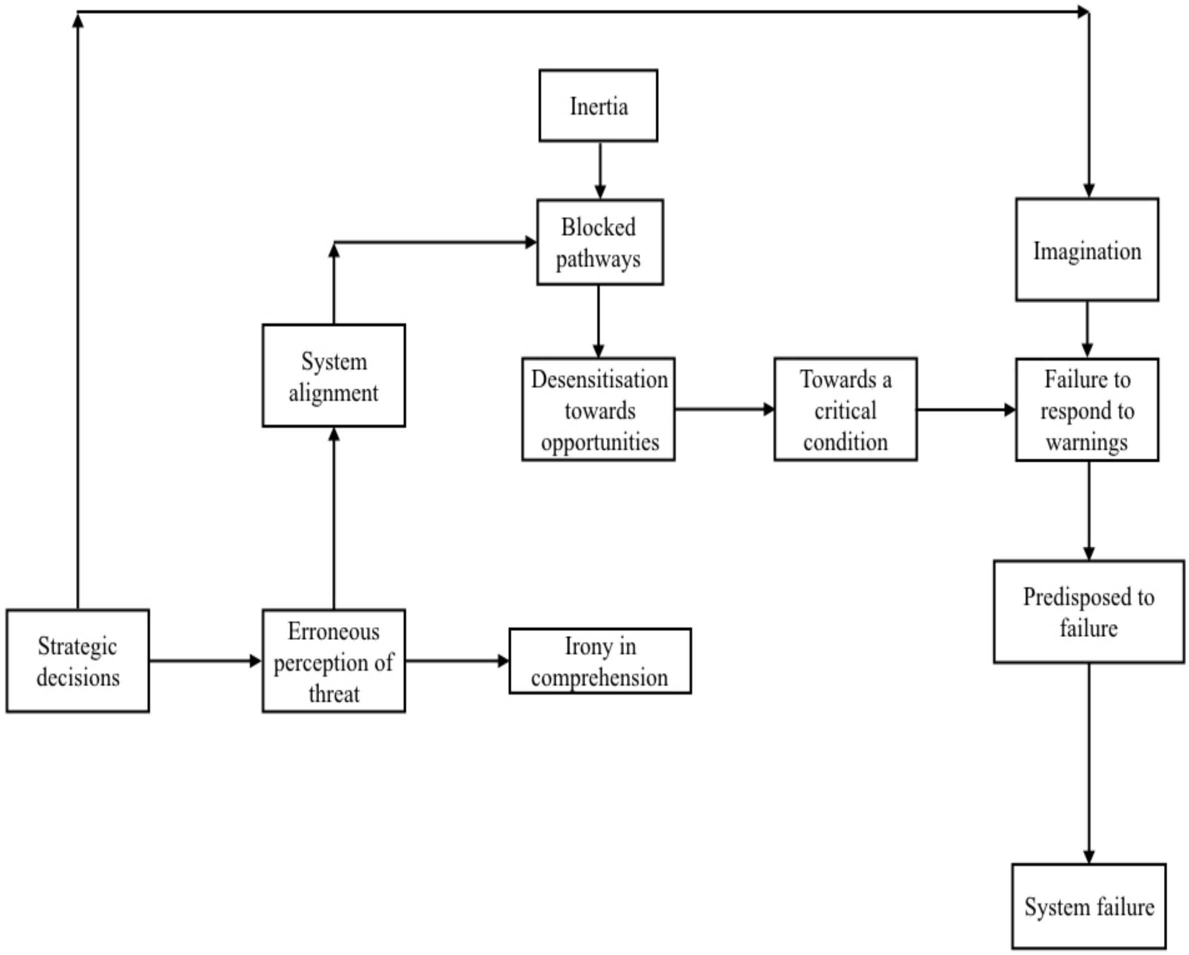

Figure 1: Linkages between main and subsidiary themes

3.1. Erroneous perception of threat

In terms of understanding how modes of failure in a real-world system are created, this first theme captures an important point. Before, and during the build-up to 9/11, the system had an erroneous perception of the threat it was facing. This perception was constructed in the strategic layers, by high-level decision-makers (e.g., the Federal Aviation Administration (FAA) who were influenced by the outcome of the 1996 Presidential Commission on aviation safety and security). The strategic decisions made by the Presidential Commission and FAA were found to be significant in creating a system that was inevitably going to fail. The erroneous perception was actualised and embedded in international legislation, FAA policy and system operating procedures. The FAA arbitrarily applied this erroneous perception—defining the objective and the operating parameters of the system.

3.2. System alignment

This theme, related to erroneous perception of threat, captures a salient point pertinent to the objectives and alignment of the security system towards the danger. In the distant context, the system perceived the risk as relating to conventional (non-suicide) hijackings and the concealment of explosive devices in baggage placed in the hold of aircraft. However, the reality was that the actual threat was somewhat different—connected to strategic plans for 'suicide' hijackings by the Islamist terrorist organisation al-Qaeda. The disparity in the alignment of the system between the perceived and real threats was also consequential to the strategic direction provided by FAA policymakers and the decisions made by the FAA's leadership.

Albeit fragmented across a large and complex structure, a collective experience was that information relating to the real threat posed by al-Qaeda, was already in existence in the system for many years before 9/11. Although these data indicate that this was the case, the threat was neither recognised nor understood. It was not perceived as being sufficiently significant to change the alignment of the system towards the new danger of Islamist suicide hijackings. The report remarks about the volume of information entering the security system and that, in some cases, it was specific about the threat of a suicide attack.

3.3. System inertia

In terms of understanding how modes of failure incubate in real-world systems, this, and the following other themes provide a further level of insight as to why the system did not understand the real threat. The size, scale and complexity of the system created inertia: where the system was unable to quickly change and respond to new information relating to other threats. These data also suggest that inertia was the outcome of dysfunctional relationships between the various human and technical elements—primarily, the CIA and FBI. This inertia made it very difficult for the system to change any previously held beliefs or perceptions about the threat posed by al-Qaeda.

3.4. Blocked information pathways

Despite attempts to achieve a more desirable condition, the flow of information in the system was far from perfect. It was laden with inherent flaws, contributory to the system not identifying and mitigating the threat. When the system was processing information, it was common for those involved, to experience information-sharing pathways to be blocked. Specifically, between the various agencies concerned in the collection of intelligence (i.e., CIA, and those involved in evidential investigations, i.e., FBI). This condition of the critical information pathways being blocked directly impacted on the capability of the FAA to contextualise information against the bigger picture and, more importantly, assess threats pertinent to the presence of al-Qaeda terrorists in the United States.

3.5. Desensitisation towards opportunities

These data suggest that the system was desensitised towards opportunities that, if acted upon, could have, at the very least provided a prospect to disrupt the plot. The report talks about these opportunities. As information about the possibility of some form of attack involving civil aviation increased, the system appears to become less sensitive to recognise the significance of critical events. For example, the arrest of Zacarias Moussaoui in August 2001 while doing flight training in the United States. After Moussaoui was arrested for immigration offences, the FBI started an intelligence investigation, and further significant information was entered into the system. This specific information did not sensitise the system to the real risk and, as a consequence, the information was not disseminated across agencies. The report identifies that there were many opportunities for the system to be sensitive to the significance of intelligence reporting about Moussaoui and other important events.

3.6. Towards a critical condition

The analysis reveals that the security system had, over time, morphed into what can be described as a critical and exploitable condition. It is interesting that, in hindsight, these data indicate the system was clearly in an unsafe condition, but at that time believed it was effectively mitigating the agreed perceived threat. The criticality of the situation was highlighted by data which suggests that the system was “blinking red” (National Commission on Terrorist Attacks upon the United States, 2004a); warning about the real threat. The interdependent human elements of the system (i.e., U.S. government; the intelligence agencies; the FAA) did not at that time recognise the significance of the information and intelligence reporting. The consequences of not attributing an appropriate level of significance to the information were that the system weakened into a dangerous condition.

3.7. Imagination

The report acknowledges the bias associated with viewing events in hindsight. Nevertheless, it comments that many of the warnings available to the system—the real threat—should have in some ways been visible in foresight and preventable. Despite this criticism, there is evidence of the specific threat of suicide hijackings being imagined by various human elements in the system. However, these key events were not visible because high-level strategic decisions, made by both politicians and agency leaders, lacked the necessary imagination to understand the potential threat.

3.8. Failure to respond to warnings

The system failed to respond to many warnings. If the threat, was imagined in the way that some senior figures describe; then the system should have understood the significance of information relating to the warnings about al-Qaeda. The fact this did not happen and that the system failed to respond to the warnings, was a telling sign of the warnings not being understood.

4. Discussion

The systems failure model for aviation security (see Figure 2) captures the fundamental relationships between each of the themes. It also considers how these general themes might interconnect and be linked. It proposes the emergence of a complex type of behaviour, where future systems may become predisposed to failure. The main components of the model are defined as follows:

1. *System cognition*: signifies the human-like practices that the system adopts to process and understand information, knowledge and past experiences, which are readily available to make decisions about risk and hazards;

2. *Erroneous perception*: refers to the skewed perception of threat that is unavoidably constructed by the system concerning how it perceives the system will fail;

3. *Configuration:* applies to how the system organisation, and its alignment towards the threat. It includes the system objectives and operating parameters for the feedback loops, and sets the level of dissonance between the perceived and real threat;

4. *Negative reinforcement*: denotes the behaviour of the negative feedback loop, which reinforces the erroneous perception and desensitises the system to the disturbances associated with the build-up of the conditions that are causal to a system failure;

5. *Positive drift:* relates to the situation where, system configuration to an erroneous perception, the negative feedback loop behaves like the positive loop. Th precis allows the precipitating conditions to accumulate and move the

system towards an unstable condition;

6. *Desensitisation:* conveys the notion that the system is unable to appreciate the significance of the information and warnings that are generated by key system events;

7. *Technological dependence*: implies the existence of a variable that is contributory to a perpetual and culturally unavoidable cycle of increasing risk and complexity in the system;

8. *Non-linear conjunction*: refers to the random and stochastic interaction between the parts and system elements and that, relating to the interaction between the conditions causal to modes of failure;

9. *Forewarning*: concerns the information made available to the system to warn of impending failure; and

10. *Emergence:* signifies the resultant behaviour of the system that makes it predisposed to failure. This emergence is consequent to the accumulation of the non-linear interactions between the system elements.

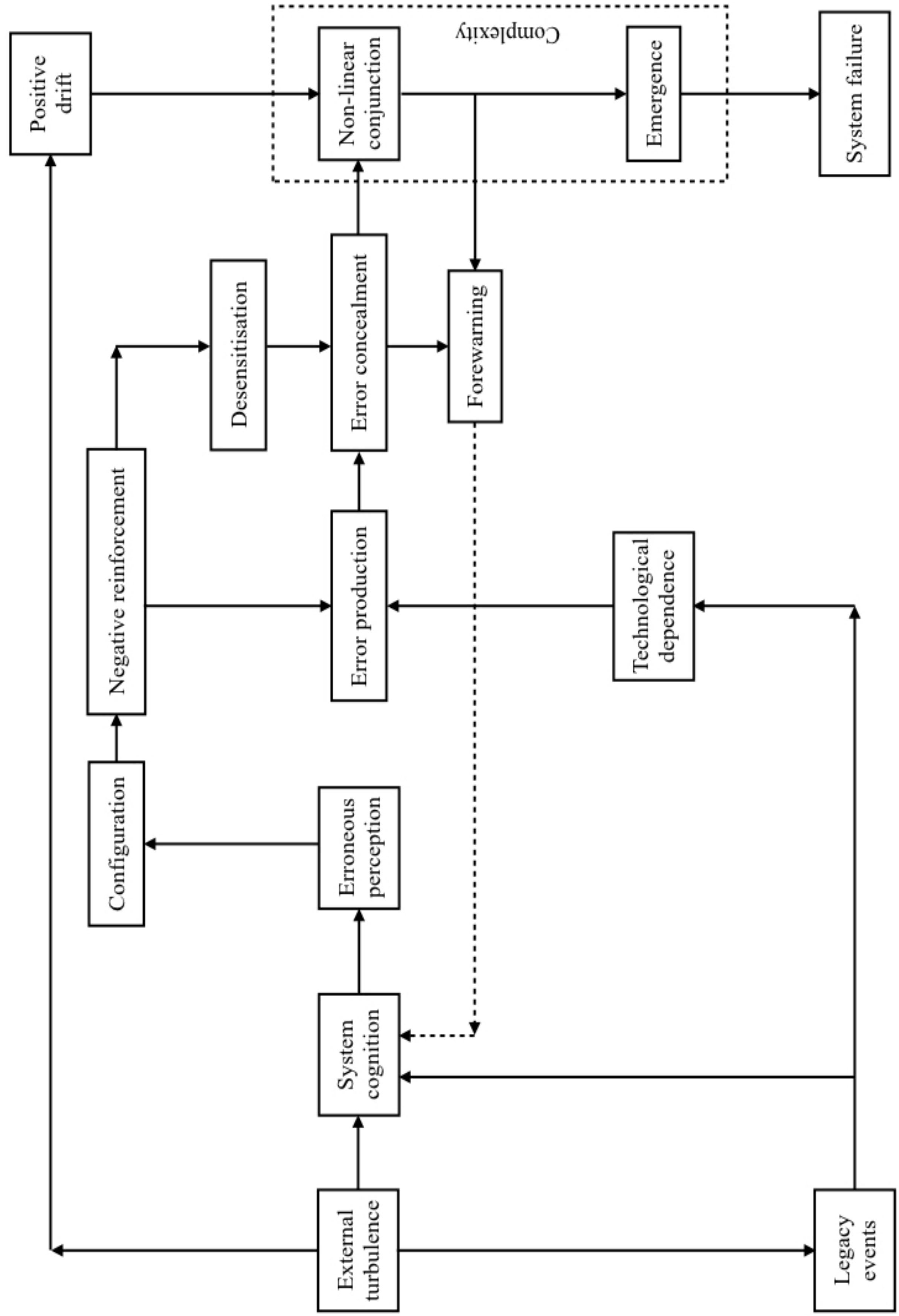

Figure 2: The systems failure model for aviation security

The model in Figure 2 proposes some form of ‘external turbulence’ where the ‘system cognition’ will use available information (including that which is biased and amplified), to construct an ‘erroneous perception’ of the threat. This ‘erroneous perception’ will directly influence the ‘configuration’ and ‘alignment’ of the system. Following ‘external turbulence’, another input which appears to play a part in determining the system’s perception of threat is the information relating to ‘legacy events' and parameters for the feedback loops. The system's responses to ‘legacy events' and ‘technological dependence' are further significant inputs.

The behaviour of the feedback loops, which generate either ‘negative reinforcement' or ‘positive drift', is linked to the introduction of modes of failure into the system. ‘Negative reinforcement' causes ‘desensitisation' and creates a further condition where modes of failure, once produced, can incubate and become concealed in the layers of the system. ‘Positive drift’ actively moves the system towards a critical condition. The ‘non-linear’ conjunction of system elements and modes of failure causes disturbances which, if recognised and understood by the ‘system cognition’, can provide ‘forewarning’ of ‘emergence’ towards unpredictable behaviour and potential system failure. Now discussed further are some of the fundamental components of the model.

4.1. External turbulence

Systems define their own beliefs about the surrounding world and perceived hazards (Turner, 1976). In aviation security, this will be where the system constructs its perception of the threat of failure. For instance, where it defines the operating objectives required to defend itself from exploitation by terrorists or other threat groups. This activity may occur at any time in the system's life but is generally at the inception of a change to the system's operation and objectives after a significant event (Turner, 1976) or some other form of ‘external turbulence’ in the operating environment.

The main themes capture those data relating to why the system was oriented towards a skewed perception of the threat. This occurrence was consequential to how high-level decision-makers processed information that was readily available to the system at that time. In particular, having completed extensive consultation with so-called experts, the 1996 Presidential Commission, concluded the prevailing threat to aviation security was conventional sabotage and placing of explosive devices onto aircraft. The effect of these high-level decisions was that the system was misaligned and did not in any way consider the real potential for system failure, from al-

Qaeda suicide hijackers.

4.2. System cognition

The concept of 'system cognition' can be used to describe the security system as being endowed with almost human-like cognition. That is processing and seeking to understand available information and past experiences to make decisions and take corrective action concerning perceived risk and hazards. Like human beings, 'system cognition' can be responsible for constructing an 'erroneous perception' of threat and two abstract but, related, system states; (i) the perceived system state, and (ii) the real system state. The findings suggest that the perceived system is homeostatic (i.e., it always returns to equilibrium); reinforced by a negative feedback loop which regulates the system to a constant state.

The real system, however, is continuously changing condition over time. Unless controlled the—positive feedback loop—will move the system away from equilibrium towards a vulnerable state at risk of failure. Although the two states are living side-by-side, they are opposed. Reconciling these states is challenging because of the difficulties of processing new information that may be at odds with the perceived system state. The outcome is the creation of a malign condition, where the constructed appreciation was some distance from the real threat.

4.3 Configuration towards the perceived threat

The perception of threat and the configuration of the system is pertinent to the creation of modes of failure. In the case study, some of these conditions, which were directly consequent to high-level decision-making, had remained dormant and undetected for many years. For example, because their profiles suggested a flight safety risk, the Computer Assisted Passenger Pre-screening System (CAPPS) selected more than half (ten) of the nineteen hijackers. In the specific case of American Airlines flight 77 at Washington Dulles Airport, the CAPPS system had selected five out the six hijackers for further investigation. The CAPPS selection only led to their checked-in (hold) luggage being screened for explosives and being held off the aircraft until they had boarded. It did not, and would not have led to any further intrusive checking of their hand luggage. This further screening, as we later learned, may have prevented the hijackers from boarding the aircraft with weapons.

In this case, these findings provide another example of a malign state which was relevant to how the terrorists were able to board the planes with box cutters and knives. This malign state was because the high-level decision-makers in the FAA prescribed a set of rules that were ambiguous and not explicit in prohibiting the carriage of knives under four inches long. Further, proposals to ban all knives and cutting implements were rejected because of the frequency of innocent alarm activations. The difficulties of detecting these items had increased passenger congestion at the checkpoints. The ambiguity of this direction created a harmful condition where some independent airlines acted to the contrary and explicitly permitted the carriage of these type of weapons in their operations guide.

The effect of this policy, when the terrorists successfully passed through the passenger screening checkpoint and boarded American Airlines flight 77, was realised. At the checkpoint, four of the terrorists set off the first metal detector alarm. Two of the same four then set off the second metal detector alarm and were searched using the hand-wand. The security operators failed to resolve the cause of the alarm activations. CCTV later identified one of the hand-searched terrorists carrying an unidentified item in his back pocket. We have been led to believe that there have been significant improvements in the system. Nevertheless, these examples illustrate the inherent flaws relating to human imperfectability, and the difficulty, therefore, of building an infallible system.

4.4 Forewarning of system failure

A central idea of this paper is that system disturbances relating to key events should be thought of as providing ‘forewarning' of the accumulation of malign conditions that create modes of failure (Ibrahim *et al.*, 2002). The configuration and alignment of the system determine whether these disturbances are detected; and whether the system regulates itself back to normal operation. Concealed modes of failure occur because the system, based on its assumptions and beliefs, attributes an incorrect level of significance to their importance (Pidgeon and O’Leary, 2000; Turner, 1978; Turner and Pidgeon, 1997). For the correct level of significance to be attributed to these events, the system needs to be told, or learn how to develop higher levels of sensitivity and awareness (Ibrahim *et al.*, 2002). This cognition is necessary to adjust the system from what it perceives; towards real-world hazards, it needs to contend with. The size and scale of the aviation security system make it very difficult (while it is operating) to change embedded beliefs or perceptions about the threat or perceived modes of failure.

From a socio-technical point of view, this is an example of what may happen when the human, technological and organisational elements are not optimised to adjust to the changing external environment. Optimisation of the socio-technical system is a critical variable. It explains why important events are not identified at the time and why elements of the system may become desensitised towards opportunities to prevent failure. It follows that a correctly optimised system could have a higher capacity to recognise the significance of warming events. Moreover, it may, therefore, be able to mitigate the creation of conditions that ultimately precipitate and initiate system failure.

4.5. Desensitisation

The theme 'desensitisation towards opportunities' captures one instance in particular, where optimisation affected the capacity of the system to recognise the significance of the arrest of Zacarias Moussaoui in August 2001. The report states that, had Bin Laden been aware of the arrest of Moussaoui, he may have cancelled the whole operation. This was important because Moussaoui was sent by al-Qaeda to the United States to train as one of the pilots. He went to the same flight training school in Oklahoma attended by other 9/11 pilots, Mohammed Atta and Marwan al-Shehhi. Suspiciously, he told the flight instructors that he did not want to learn to fly Boeing 747, but only wanted to learn how to take off and land. The flight school reported this unusual behaviour to the authorities. Nevertheless, he was only arrested for immigration offences by the Immigration and Naturalization Service (National Commission on Terrorist Attacks upon the United States, 2004b).

Before the arrest of Moussaoui in August 2001, there was much information in the system about the risk posed by students being sent by Bin Laden to attend flight training schools in Arizona. An FBI Agent in the Phoenix field office sent a memo to Washington warning of the possibility of coordinated effort to send students to learn to fly in the United States. The same agent made a series of recommendations to develop the intelligence picture around Moussaoui—none of which were acted upon in advance of 9/11 (National Commission on Terrorist Attacks upon the United States, 2004b).

Significantly, having been told of the circumstances relating to the arrest of Moussaoui, the CIA did not recognise any connection with al-Qaeda and therefore did not discuss the matter further. Albeit, one day later, the CIA sent a communication to London regarding "subjects involved in suspicious 747 flight training" and described Moussaoui as a "possible suicide hijacker"—the system—made "no connection [...] between Moussaoui's presence in the

United States and the threat reporting during the summer of 2001" (National Commission on Terrorist Attacks upon the United States, 2004b). While this information may not have uncovered the plot, the Commission did accept that it may have sensitized the FBI to take the arrest of Moussaoui more seriously.

4.6. The inevitability of system failure

Perrow (1999) in his widely accepted analysis of system failures explains that "nothing is perfect; every part of every system […] is liable to failure." If within a system, the characteristics of interactive complexity and tight coupling co-exist, then there can be a normal system accident. That is a system failure that, because of random and unexpected interactions of non-critical and unremarkable events; it cannot be prevented or designed-out by engineers (Downer, 2010).

Perrow (1999) focuses on two types of interactions that go some way to answer the question as to whether aviation security failures are inevitable. Firstly, linear interactions are those expected by everybody when the system is operating with clearly defined sequences and process. Secondly, complex interactions, on the other hand, are those not intended during the system design. They have their genesis in parts of the system that perform more than one function. These data suggest the interactions between many of the interdependent but unrelated systems and sub-systems are complex. Even though warning information was present in the system, the system did not anticipate the interactions. The capacity to anticipate did not occur because (as previously stated) the perception of threat did not consider the real potential for system failure.

Similarly, these findings imply the system did not anticipate the interactions between the various foreign and domestic intelligence agencies would also be complex. Moreover, it did not anticipate these interactions being causal to critical information not being shared, collectively analysed and understood, or acted upon in a timely way to disrupt the plot. The system expected the agencies would be using agreed linear processes and protocols and would work in tandem towards a collective objective of sharing information across the foreign and domestic threshold. These data also explicitly state that the lack of imagination by high-level decision-makers was significant in the failure of the system. In this sense, neither the literature nor these data are clear about whether the idea of system imagination can be relied upon to identify the importance of critical events and interactions.

4.7. Technological dependence

Stricter regulatory control was realised in many ways, but most significantly by reliance on further complex technological solutions to mitigate the perceived risk to the system. For example, after 9/11, the governmental policy led to a "multibillion-dollar investment in homeland security" (Harvey, 2006) and an increasing dependence upon complex technological solutions. This dependence on technological countermeasures is evident in response to each of the significant terrorist events since 9/11, such as; Richard Reid - The Shoe Bomber (2001), Bojinka II - Operation Overt - The Liquid Bomb Plot (2006), Umar Farouk Abdulmutallab - The Underpants Bomber (2009), Operation Hemorrhage - The Printer Cartridge Plot (2010), and The Explosive Plot (2012).

These events reveal a discernible pattern where, over the years, more and more complicated technologies have been relied upon to defend the system. For example, the 9/11 passenger screening checkpoint has now been extended to include, amongst other technologies, full-body scanners and automated explosive trace detection systems. There is nothing to suggest that the anticipatory and preventative effect of these methods has reduced system failures. The literature implies that technological dependence creates a paradox: where in seeking to strengthen defences, system interactions become actively more complex and difficult to predict.

4.8. Negative Reinforcement and positive drift

System feedback loops can fabricate conditions for creating modes of failure. For example, the lack of imagination of failure is a negative loop reinforcing the erroneous perception. The drift created by the positive loop (allowing the creation and incubation of modes of failure) is ultimately related to the unnoticed system failure. Positive drift moves the system towards a critical condition. For example, in the case study, the strategic decision-makers failed to correctly assimilate and understand available intelligence about the real threat of suicide hijacking. This action led to the failure to recognise the significance of the arrest of Moussaoui in August 2000 and the failure to detect the routine and deliberate violations by passenger security operators at Washington-Dulles and other airports. In this case, an unusual condition was found to exist. At the time of operation, the system was doing what it perceived to be correct. Nevertheless, when in possession of the after-event information—what the system was doing is now considered to be wrong. Further, the negative feedback loop regulating system behaviour was—in hindsight—performing the function of the positive feedback loop—creating conditions for the system to fail.

This paper proposes that in this complicated situation, the system—in foresight—will find it challenging to be cognisant of vulnerabilities not associated with the perceived and expected threat. While the system only corrects activity relating to the perceived threat, it can unknowingly move into a critical condition; forming modes of failure through the defensive layers of the system. This complex emergent behaviour will be unavoidable unless the system is correctly re-configured to include an expectation of emerging real threats. Alternatively, it becomes sensitised in such a way to detect all relevant disturbances that might amount to a new threat. In this setting, the system, rather than being predictive, is weighted towards being predisposed to inevitable failure.

4.9. Aviation security as a complex socio-technical system

The notion that aviation security can be thought of as a complex system is an interesting contribution. Applying this type of approach to aviation security provides a greater understanding of how unique elements interact in isolation and together with other parts of the system (Hoyland and Aase, 2009). Analysing aviation security failures in this way has the practical benefit of providing a further level of insight that hitherto has been unavailable to security practitioners and academics. Furthermore, complexity is an appropriate theoretical lens because these data suggest that aviation security consists of many parts that interact to develop unpredictable system behaviour (Marion and Uhl-Bien 2001; Marion and Uhl-Bien 2003; Regine and Lewin 2000). Also, this study indicates that the aviation security system demonstrates macroscopic emergent behaviour, which is difficult for the system to predict. Figure 5-12 highlights the part of the model that is associated with complex behaviour.

5. 0. Conclusions

In summary, the systems failure model for aviation security proposes 'system cognition' will construct an 'erroneous perception' of threat, influencing the 'configuration' and alignment of the system. Together with the response to 'legacy events', and 'technological dependence' these become significant inputs in the number of errors that are produced and left untreated by the system. The feedback loops generate 'negative reinforcement' and 'positive drift', which are contributory to the incubation and concealment of modes of failure. Importantly, the model proposes the ‘complex’ interactions cause disturbances which provide ‘forewarning’ of the system producing emergent and unpredictable behaviour where it can fail at any time. The model proposes the alignment of the system may be related to the information and the warnings not being understood.

The systems failure model for aviation security also illustrates how the general concepts may be linked. It demonstrates also how the concepts can be applied to explain why the aviation security system can become predisposed to failure. The findings from the study explain that system optimisation is an essential variable in the model. This variable can also be used to understand why the system becomes desensitised towards opportunities to configure itself towards the real threat. Therefore, for the reasons discussed, more formal methods should be sought to identify, understand and predict the significance of interactions causal to system failure. For example, the quantitative risk modelling framework developed by Iervolino et al. (2019) could be extended to predict the annual fatality risk of aviation security failures. These data could be combined with the conceptual ideas proposed by the systems failure model to provide new empirical insights.

The model is limited because it relates only to the events of 9/11. Nevertheless, security practitioners and academic researchers can still use the model to inform future policy-making decisions. Further, given that this study is nascent, future research should also endeavour to identify interventions that warns and aligns the system to the ever-changing threat of exploitation.

References:

Aini, M. S., Fakhrul-Razi, A., 2010. Development of socio-technical disaster model. Safety Science 48, 1286–1295.

Boyatzis, R. E., 1998. Transforming qualitative information: Thematic analysis and code development. Sage Publications, Thousand Oaks, CA.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qualitative Research in Psychology 3, 77-101.

Crabtree, B. F., Miller, W. L., 1999. Doing Qualitative Research. Sage Publications, Thousand Oaks, CA.

Downer, J., 2010. Anatomy of a disaster: Why some accidents are unavoidable. London School of Economics: Centre for analysis of risk and regulation. http://eprints.lse.ac.uk/36542/1/Disspaper61.pdf (July 18 2019).

Fereday, J., Muir-Cochrane, E., 2006. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. Qualitative methods 5, 1–11.

Gilbert, N., 2008. Researching social life. Sage Publications, London.

Harvey, F., 2006. The homeland security dilemma: The imaginations of failure and the escalating costs of perfect security. Canadian Journal of Political Science 40, 283-316.

Hoyland, S., Aase, K., 2009. Does change challenge safety? Complexity in the civil aviation transport system. In: Martorell, S., Soares, C. G., Barnett, J., (Eds.), Safety, reliability and risk analysis. Theory, methods and applications. pp.1385–1394.

Ibrahim, M. S., Fakhru'l-Razi, A., Sa'ari, M., Aini, M. S., Rashid, S. 2002. Bright sparklers fire and explosions: The lessons learned. International Journal of Disaster Prevention and Management 11, 214-221.

International Civil Aviation Organisation. 2011. Security: Safeguarding international civil aviation against acts of unlawful interference. Annex 17 to the convention on international civil aviation. International Civil Aviation Organisation, Montreal.

Iervolino, I., Accardo, D., Tirri, A.E., Pio, G., Salzano,E. 2019. Quantative risk analysis for the Amerigo Vespucci (Florence, Italy) airport including domino effects. Safety Science 113, 472-498.

Jenkins, B., 2012. Aviation security: After four decades, it's time for a fundamental review. RAND Corporation, Santa Monica.

King, N., 2004. Using templates in the thematic analysis of text. In: Cassell, C., Symon, G. (Eds.), Essential guide to qualitative methods in organizational research. Sage Publications, London.

LaTourrette, T., Jenkins, B., 2012. The goal of efficient security. In: Jackson, B., LaTourrette, T., Chan, E., Lundberg, R., Morral, A., Frelinger, D. (Eds.) Efficient aviation security: Strengthening the analytic foundation for making air transportation security decisions. https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1220.sum.pdf (July 18 2019).

Marion, R., Uhl-Bien, M., 2001. Leadership in complex organizations. Leadership Quarterly 12, 389–418.

Marion, R., Uhl-Bien, M., 2003. Complexity theory and Al-Qaeda: Examining complex leadership. Emergence 5, 54-76.

McDonald, K., 2001. Social documents. In: Gilbert, N. (Eds.) Researching social life. 2nd edn. Sage Publications, London.

National Commission on Terrorist Attacks upon the United States 2004a. The 9/11 Commission Report. W.W. Norton & Company, New York.

National Commission on Terrorist Attacks upon the United States 2004b. The 9/11 Commission Report: Executive summary.
https://govinfo.library.unt.edu/911/report/911Report_Exec.pdf (July 18 2019).

Perrow, C., 1999. Normal accidents: Living with high risk technologies. Princeton University Press, New Jersey.

Pidgeon, N., O'Leary, M., 2000. Man-made disasters: Why technology and organizations (sometimes) fail. Safety Science 34, 15–30.

Reason, J., 1990. Human error. Cambridge University Press, New York.

Reason, J., 2008. The human contribution: Unsafe acts, accidents and heroic recoveries. Ashgate Publishing Limited, Farnham.

Regine, B., Lewin, R., 2000. Leading at the edge: How leaders influence complex systems. Emergence 2, 5–23.

Riley, K. J., 2011. Air travel security sine 9/11. RAND Corporation, Santa Monica.

Roulston, K., 2001. Data analysis and theorizing as ideology. Qualitative Research. 1, 279-302.

Toft, B., Reynolds, S., 1999. Learning from disasters: A management approach. Perpetuity Press, London.

Toft, B., Reynolds, S., 2005. Learning from disasters: A management approach. 2nd edn. Butterworth Heinemann, London.

Turner, B. A., 1976. The development of disasters: A sequence model for the analysis of the origin of disasters. Sociological Review 24, 753–775.

Turner, B. A., 1978. Man-made disasters. Wykeham Publications, London.

Turner, B. A., Pidgeon, N.F., 1997. Man-made disasters. 2nd edn. Butterworth-Heinemann, London.

Waring, T., Wainwright, D., 2008. Issues and challenges in the use of template analysis: Two comparative case studies from the field. The Electronic Journal of Business Research Methods 6, 85-94.

Weigman, D, A., Shappell, S, A., 1997. Human factors analysis of post-accident data: Applying theoretical taxonomies of human error. The International Journal of Aviation Psychology 7, 67-81.

Yin, R. K., 2009. Case study: Research, design and methods. Sage Publications, London.

Appendices:

Appendix A:

Extracts from the TCA used to support each theme.

Theme 1: Erroneous Perception of Threat

President Clinton created a commission under Vice President Al Gore to report on shortcomings in aviation security in the United States. The Gore Commission's report, having thoroughly canvassed available expertise in and outside of government, did not mention suicide hijackings or the use of aircraft as weapons. It focused mainly on the danger of placing bombs onto aircraft—the approach of the Manila air plot. The Gore Commission did call attention, however, to lax screening of passengers and what they carried onto planes (ENU344, 2004a).

President Al Gore reinforced the prevailing concern about sabotage and explosives on aircraft. The Gore Commission also flagged, as a new danger, the possibility of attack by surface-to-air missiles. Its 1997 final report did not discuss the possibility of suicide hijackings (ENU82, 2004a).

The Federal Aviation Administration (FAA) within the Department of Transportation had been vested by Congress with the sometimes-conflicting mandate of regulating the safety and security of U.S. civil aviation while also promoting the civil aviation industry. The FAA had a security mission to protect the users of commercial air transportation against terrorism and other criminal acts. In the years before 9/11, the FAA perceived sabotage as a greater threat to aviation than hijacking. First, no domestic hijacking had occurred in a decade. Second, the commercial aviation system was perceived as more vulnerable to explosives than to weapons such as firearms. Finally, explosives were perceived as deadlier than hijacking and therefore of greater consequence (ENU82, 2004b).

In early August 1999, the FAA's Civil Aviation Security intelligence office summarized the Bin Ladin hijacking threat. After a solid recitation of all the information available on this topic, the paper identified a few principal scenarios, one of which was a suicide hijacking operation. The FAA analysts judged such an operation unlikely, because it does not offer an opportunity for dialogue to achieve the key goal of obtaining Rahman and other key captive extremists. A suicide hijacking is assessed to be an option of last resort (ENU345, 2004a).

The tragedy of the embassy bombings provided an opportunity for a full examination, across the government, of the national security threat that Bin Ladin posed. Such an examination could have made clear to all that issues were at stake that were much larger than the domestic politics of the moment. Nevertheless, the major policy agencies of the government did not meet the threat (ENU349, 2004).

While FAA rules did not expressly prohibit knives with blades under 4 inches long, the airlines' checkpoint operations guide (which was developed in cooperation with the FAA), explicitly permitted them. The FAA's basis for this policy was (1) the agency did not consider such items to be menacing, (2) most local laws did not prohibit individuals from carrying such knives, and (3) such knives would have been difficult to detect unless the sensitivity of metal detectors had been greatly increased. A proposal to ban knives altogether in 1993 had been rejected because small cutting implements were difficult to detect and the number of innocent 'alarms' would have increased significantly, exacerbating congestion problems at checkpoints (ENU84, 2004a).

Several years prior to 9/11, an FAA requirement for screeners to conduct 'continuous' and 'random' hand searches of carry-on luggage at checkpoints had been replaced by explosive trace detection or had become ignored by the air carriers. Therefore, secondary screening of individuals and their carry-on bags to identify weapons (other than bombs) was non-existent, except for passengers who triggered the metal detectors. Even when small knives were detected by secondary screening, they were usually returned to the traveller. Reportedly, the 9/11 hijackers were instructed to use items that would be undetectable by airport checkpoints (ENU84, 2004b).

The second part of pre-screening called on the air carriers to implement an FAA-approved computerized algorithm (known as CAPPS, for Computer Assisted Passenger Pre-screening System) designed to identify passengers whose profile suggested they might pose more than a minimal risk to aircraft. Although the algorithm included hijacker profile data, at that time only passengers checking bags were eligible to be selected by CAPPS for additional scrutiny. Selection entailed only having one's checked baggage screened for explosives or held off the airplane until one had boarded. Primarily because of concern regarding potential discrimination and the impact on passenger throughput, "selectees" were no longer required to undergo extraordinary screening of their carry-on baggage as had been the case before the system was computerized in 1997. This policy change also reflected the perception that non suicide sabotage was the primary threat to civil aviation (ENU84, 2004c).

The final layer, security on board commercial aircraft, was not designed to counter suicide hijackings (ENU85, 2004a).

The strategy operated on the fundamental assumption that hijackers issue negotiable demands (most often for asylum or the release of prisoners) and that, as one FAA official put it, 'suicide wasn't in the game plan' of hijackers (ENU85, 2004b).

Theme 2: System Alignment

The FAA's policy was to use intelligence to identify both specific plots and general threats to civil aviation security, so that the agency could develop and deploy appropriate countermeasures. The FAA's 40-person intelligence unit was supposed to receive a broad range of intelligence data from the FBI-, CIA-, and other agencies so that it could make assessments about the threat to aviation. However, the large volume of data contained little pertaining to the presence and activities of terrorists in the United States. For example, information on the FBI's effort in 1998 to assess the potential use of flight training by terrorists and the Phoenix electronic communication of 2001 warning of radical Middle Easterners attending flight school were not passed to FAA headquarters. Several top FAA intelligence officials called the domestic threat picture a serious blind spot (ENU83, 2004a).

Moreover, the FAA's intelligence unit did not receive much attention from the agency's leadership. Neither Administrator Jane Garvey nor her deputy routinely reviewed daily intelligence, and what they did see was screened for them. She was unaware of a great amount of hijacking threat information from her own intelligence unit, which, in turn, was not deeply involved in the agency's policymaking process (ENU83, 2004b).

The protocols in place on 9/11 for the FAA and NORAD to respond to a hijacking presumed that the hijacked aircraft would be readily identifiable and would not attempt to disappear; that there would be time to address the problem through the appropriate FAA and NORAD chains of command; and that the hijacking would take the traditional form: that is, it would not be a suicide hijacking designed to convert the aircraft into a guided missile. On the morning of 9/11, the existing protocol was unsuited in every respect for what was about to happen (ENU18, 2004).

Although the FAA had authority to issue security directives mandating new security procedures, none of the few that were released during the summer of 2001 increased security at checkpoints or on-board aircraft. The information circulars mostly urged air carriers to "exercise prudence" and be alert. Prior to 9/11, the FAA did present a CD-ROM to air carriers and airport authorities describing the increased threat to civil aviation. The presentation mentioned the possibility of suicide hijackings but said that 'fortunately, we have no indication that any group is currently thinking in that direction'. The FAA conducted 27 special security briefings for specific air carriers between May 1, 2001, and September 11, 2001. Two of these briefings discussed the hijacking threat overseas. None discussed the possibility of suicide hijackings or the use of aircraft as weapons. No new security measures were instituted (ENU264, 2004).

On Friday, December 4, 1998, the CIA included an article in the Presidential Daily Brief describing intelligence, received from a friendly government, about a threatened hijacking in the United States. This article was declassified at our request. […]. Redacted material is indicated in brackets.

SUBJECT: Bin Ladin Preparing to Hijack US Aircraft and Other Attacks

1. Reporting [—] suggests Bin Ladin and his allies are preparing for attacks in the US, including an aircraft hijacking to obtain the release of Shaykh 'Umar 'Abd al-Rahman, Ramzi Yousef, and Muhammad Sadiq 'Awda. One source quoted a senior member of the Gama'at al-Islamiyya (IG) saying that, as of late October, the IG had completed planning for an operation in the US on behalf of Bin Ladin, but that the operation was on hold. A senior Bin Ladin operative from Saudi Arabia was to visit IG counterparts in the US soon thereafter to discuss options—perhaps including an aircraft hijacking.

1. IG leader Islambuli in late September was planning to hijack a US airliner during the 'next couple of weeks' to free 'Abd al- Rahman and the other prisoners, according to what may be a different source. The same source late last month said that Bin Ladin might implement plans to hijack US aircraft before the beginning of Ramadan on 20 December and that two members of the operational team had evaded security checks during a recent trial run at an unidentified New York airport.

2. Some members of the Bin Ladin network have received hijack training, according to various sources, but no group directly tied to Bin Ladin's al-Qa'ida organization has ever carried out an aircraft hijacking. Bin Ladin could be weighing other types of operations against US aircraft. According to [—] the IG in October obtained SA-7 missiles and intended to move them from Yemen into Saudi Arabia to shoot down an Egyptian plane or, if unsuccessful, a US military or civilian aircraft. A [—] in October told us that unspecified 'extremist elements' in Yemen had acquired SA-7s.

3. [—] indicate the Bin Ladin organization or its allies are moving closer to implementing anti-US attacks at unspecified locations, but we do not know whether they are related to attacks on aircraft. A Bin Ladin associate in Sudan late last month told a colleague in Kandahar that he had shipped a group of containers to Afghanistan. Bin Ladin associates also talked about the movement of containers to Afghanistan before the East Africa bombings.

4. In other [—] Bin Ladin associates last month discussed picking up a package in Malaysia. One told his colleague in Malaysia that 'they' were in the 'ninth month [of pregnancy]'. An alleged Bin Ladin supporter in Yemen late last month remarked to his mother that he planned to work in 'commerce' from abroad and said his impending 'marriage,' which would take place soon, would be a 'surprise'. 'Commerce' and 'marriage' often are code words for terrorist attacks (ENU128129. 2004).

A June 12 CIA report passing along biographical background information on several terrorists mentioned, in commenting on Khalid Sheikh Mohammed, that he was recruiting people to travel to the United States to meet with colleagues already there so that they might conduct terrorist attacks on Bin Ladin's behalf. On June 22, the CIA notified all its station chiefs about intelligence suggesting a possible al Qaeda suicide attack on a U.S. target over the next few days (ENU256, 2004a).

Threat reports also mentioned the possibility of using an aircraft filled with explosives. The most prominent of these mentioned a possible plot to fly an explosives-laden aircraft into a U.S. city (ENU344, 2004b).

Theme 3: System Inertia

On December 4, 1998, DCI Tenet- issued a directive to several CIA officials and his deputy for community management, stating: ‘We are at war. I want no resources or people spared in this effort, either inside CIA or the Community’. The memorandum had little overall effect on mobilizing the CIA or the intelligence community (ENU357, 2004).

The domestic agencies never mobilized in response to the threat. They did not have direction, and did not have a plan to institute. The borders were not hardened. Transportation systems were not fortified. Electronic surveillance was not targeted against a domestic threat. State and local law enforcement were not marshalled to augment the FBI’s efforts. The public was not warned. The terrorists exploited deep institutional failings within our government (ENU26, 2004).

On August 22 and 27, the French provided information that made a connection between Moussaoui and a rebel leader in Chechnya, Ibn al Khattab. This set off a spirited debate between the Minneapolis Field Office, FBI headquarters, and the CIA as to whether the Chechen rebels and Khattab were sufficiently associated with a terrorist organization to constitute a foreign power for purposes of the FISA statute. FBI headquarters did not believe this was good enough, and its National Security Law Unit declined to submit a FISA- application (ENU274, 2004).

There was substantial disagreement between Minneapolis agents and FBI headquarters as to what Moussaoui was planning to do. In one conversation between a Minneapolis supervisor and a headquarters agent, the latter complained that Minneapolis’s FISA request was couched in a manner intended to get people spun up. The supervisor replied that was precisely his intent. He said he was trying to keep someone from taking a plane and crashing into the World Trade Center. The headquarters agent replied that this was not going to happen and that they did not know if Moussaoui was a terrorist (ENU275, 2004a).

On August 23, DCI Tenet was briefed about the Moussaoui case in a briefing titled ‘Islamic Extremist Learns to Fly’. Tenet was also told that Moussaoui wanted to learn to fly a 747, paid for his training in cash, was interested to learn the doors do not open in flight, and wanted to fly a simulated flight from London to New York. He was told that the FBI had arrested Moussaoui because of a visa overstay and that the CIA was working the case with the FBI. Tenet told us that no connection to al Qaeda was apparent to him at the time. Seeing it as an FBI case, he did not discuss the matter with anyone at the White House or the FBI. No connection was made between Moussaoui’s presence in the United States and the threat reporting during the summer of 2001 (ENU275, 2004b).

As mentioned above, before 9/11 the FBI agents in Minneapolis had failed to persuade supervisors at headquarters that there was enough evidence to seek a FISA warrant to search Moussaoui’s computer hard drive and belongings (ENU276, 2004).

Whatever the weaknesses in the CIA’s portraiture, both Presidents Bill Clinton and George Bush and their top advisers told us they got the picture they understood Bin Ladin was a danger. But given the character and pace of their policy efforts, we do not believe they fully understood just how many people al Qaeda might kill, and how soon it might do it. At some level that is hard to define, we believe the threat had not yet become compelling (ENU343, 2004).

Theme 4: Blocked Information Pathways

These procedures—while requiring the sharing of intelligence information with prosecutors—regulated the manner in which such information could be shared from the intelligence side of the house to the criminal side. These procedures were almost immediately misunderstood and misapplied. As a result, there was far less information sharing and coordination between the FBI and the Criminal Division in practice than was allowed under the department’s procedures.

Over time the procedures came to be referred to as ‘the wall’. The term ‘the wall’ is misleading, however, because several factors led to a series of barriers to information sharing that developed (ENU79, 2004a).

This perception evolved into the still more exaggerated belief that the FBI could not share any intelligence information with criminal investigators, even if no FISA procedures had been used. Thus, relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators. Separate reviews in 1999, 2000, and 2001 concluded independently that information sharing was not occurring, and that the intent of the 1995 procedures was ignored routinely (ENU79, 2004b).

Information was not shared, sometimes inadvertently or because of legal misunderstandings. Analysis was not pooled. Effective operations were not launched. Often the handoffs of information were lost across the divide separating the foreign and domestic agencies of the government (ENU353, 2004).

The next aviation security layer was passenger pre-screening. The FAA directed air carriers not to fly individuals known to pose a ‘direct’ threat to civil aviation. But as of 9/11, the FAA’s ‘no-fly’ list contained the names of just 12 terrorist suspects (including 9/11 mastermind Khalid Sheikh Mohammed), even though government watch lists contained the names of many thousands of known and suspected terrorists. This astonishing mismatch existed despite the Gore Commission’s having called on the FBI and CIA four years earlier to provide terrorist watch lists to improve pre-screening. The long- time chief of the FAA’s civil aviation security division testified that he was not even aware of the State Department’s TIPOFF list of known and suspected terrorists (some 60,000 before 9/11) until he heard it mentioned during the Commission’s January 26, 2004, public hearing. The FAA had access to some TIPOFF data, but apparently found it too difficult to use (ENU8384, 2004).

Theme 5: Desensitisation Towards Opportunities

In July 2001, an FBI agent in the Phoenix field office sent a memo [the ‘Phoenix memo’] to FBI headquarters and to two agents on international terrorism squads in the New York Field Office, advising of the ‘possibility of a coordinated effort by Usama Bin Ladin’ to send students to the United States to attend civil aviation schools. The agent based his theory on the ‘inordinate number of individuals of investigative interest’ attending such schools in Arizona (ENU272, 2004a).

The agent made four recommendations to FBI headquarters: to compile a list of civil aviation schools, establish liaison with those schools, discuss his theories about Bin Ladin with the intelligence community, and seek authority to obtain visa information on persons applying to flight schools. His recommendations were not acted on. His memo was forwarded to one field office. Managers of the Usama Bin Ladin unit and the Radical Fundamentalist unit at FBI headquarters were addressees, but they did not even see the memo until after September 11. No managers at headquarters saw the memo before September 11, and the New York Field Office took no action (ENU272, 2004b).

If the memo had been distributed in a timely fashion and its recommendations acted on promptly, we do not believe it would have uncovered the plot. It might well, however, have sensitised the FBI so that it might have taken the Moussaoui matter more seriously the next month (ENU272, 2004c).

August 2001: FBI headquarters does not recognise the significance of the information regarding Moussaoui’s training and beliefs and thus does not take adequate action to share information, involve higher-level officials across agencies, obtain information regarding Moussaoui’s ties to al Qaeda, and give sufficient priority to determining what Moussaoui might be planning (ENU356, 2004c).

January 2000: the CIA does not watch list Khalid al Mihdhar or notify the FBI when it learned Mihdhar possessed a valid U.S. visa (ENU356, 2004d).

January 2001: the CIA does not inform the FBI that a source had identified Khallad, or Tawfiq bin Attash, a major figure in the October 2000 bombing of the USS Cole, as having attended the meeting in Kuala Lumpur with Khalid al Mihdhar (ENU356, 2004e).

May 2001: a CIA official does not notify the FBI about Mihdhar's U.S. visa, Hazmi's U.S. travel, or Khallad's having attended the Kuala Lumpur meeting (identified when he reviewed all of the relevant traffic because of the high level of threats) (ENU356, 2004f).

August 2001: the FBI does not recognize the significance of the information regarding Mihdhar and Hazmi's possible arrival in the United States and thus does not take adequate action to share information, assign resources, and give sufficient priority to the search (ENU356, 2004g).

August 2001: the CIA and FBI do not connect the presence of Mihdhar, Hazmi, and Moussaoui to the general threat reporting about imminent attacks (ENU356, 2004h).

Theme 6: Towards a Critical Condition

The September 11 attacks fell into the void between the foreign and domestic threats. The foreign intelligence agencies were watching overseas, alert to foreign threats to U.S. interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States. No one was looking for a foreign threat to domestic targets. The threat that was coming was not from sleeper cells. It was foreign—but from foreigners who had infiltrated into the United States (ENU263, 2004).

[T]op officials reported 'Bin Ladin planning multiple operations'. When the deputies discussed al Qaeda policy on April 30, they began with a briefing on the threat (ENU255, 2004a).

In May 2001, the drumbeat of reporting grew louder with reports to top officials that 'Bin Ladin public profile may presage attack' and 'Bin Ladin network's plans advancing'. In early May, a walk-in to the FBI claimed there was a plan to launch attacks on London, Boston, and NewYork. Attorney General John Ashcroft was briefed by the CIA on May 15 regarding al Qaeda generally and the current threat reporting specifically (ENU255, 2004b).

The next day brought a report that a phone call to a U.S. embassy had warned that Bin Ladin supporters were planning an attack in the United States using 'high explosives' (ENU256, 2004b).

In the spring of 2001, the level of reporting on terrorist threats and planned attacks increased dramatically to its highest level since the millennium alert. At the end of March, the intelligence community disseminated a terrorist threat advisory, indicating a heightened threat of Sunni extremist terrorist attacks against U.S. facilities, personnel, and other interests (ENU255, 2004c).

[Moussaoui] had none of the usual qualifications for flight training on Pan Am's Boeing 747 flight simulators. He said he did not intend to become a commercial pilot but wanted the training as an 'ego boosting thing'. Moussaoui stood out because, with little knowledge of flying, he wanted to learn how to 'take off and land' a Boeing 747 (ENU273, 2004).

FBI headquarters does not recognize the significance of the information regarding Moussaoui's training and beliefs and thus does not take adequate action to share information, involve higher-level officials across agencies, obtain information regarding Moussaoui's ties to al Qaeda, and give sufficient priority to determining what Moussaoui might be planning (ENU356, 2004a).

The CIA and FBI do not connect the presence of Mihdhar-, Hazmi-, and Moussaoui to the general threat reporting about imminent attacks (ENU356, 2004b).

Theme 7: Imagination

In his testimony, Clarke commented that he thought that warning about the possibility of a suicide hijacking would have been just one more speculative theory among many, hard to spot since the volume of warnings of 'al Qaeda threats and other terrorist threats, was in the tens of thousands—probably hundreds of thousands'. Yet the possibility was imaginable, and imagined. In early August 1999, the FAA's Civil Aviation Security intelligence office summarized the Bin Ladin hijacking threat. After a solid recitation of all the information available on this topic, the paper identified a few principal scenarios, one of which was a 'suicide hijacking operation'. The FAA analysts judged such an operation unlikely, because 'it does not offer an opportunity for dialogue to achieve the key goal of obtaining Rahman and other key captive extremists […]. A suicide hijacking is assessed to be an option of last resort' (ENU345, 2004b).

Clarke's staff warned, 'Foreign terrorist sleeper cells are present in the US and attacks in the US are likely'. Clarke asked Berger to try to make sure that the domestic agencies remained alert. 'Is there a threat to civilian aircraft?' he wrote. Clarke also asked the principals in late December to discuss a foreign security service report about a Bin Ladin plan to put bombs on transatlantic flights (ENU179, 2004).

Theme 8: Failure to Respond to Warnings

These methods have been articulated in many ways, but almost all seem to have at least four elements in common: (1) think about how surprise attacks might be launched; (2) identify telltale indicators connected to the most dangerous possibilities; (3) where feasible, collect intelligence on these indicators; and (4) adopt defenses to deflect the most dangerous possibilities or at least trigger an earlier warning (ENU346, 2004).

The methods for detecting and then warning of surprise attack that the U.S. government had so painstakingly developed in the decades after Pearl Harbor did not fail; instead, they were not really tried. They were not employed to analyze the enemy that, as the twentieth century closed, was most likely to launch a surprise attack directly against the United States (ENU347348, 2004).

The CTC did not develop a set of telltale indicators for this method of attack. For example, one such indicator might be the discovery of possible terrorists pursuing flight training to fly large jet aircraft, or seeking to buy advanced flight simulators (ENU347, 2004a).

The CTC did not propose, and the intelligence community collection management process did not set, requirements to monitor such telltale indicators. Therefore, the warning system was not looking for information such as the July 2001 FBI report of potential terrorist interest in various kinds of aircraft training in Arizona, or the August 2001 arrest of Zacarias Moussaoui because of his suspicious behaviour in a Minnesota flight school. In late August, the Moussaoui arrest was briefed to the DCI and other top CIA officials under the heading 'Islamic Extremist Learns to Fly'. Because the system was not tuned to comprehend the potential significance of this information, the news had no effect on warning (ENU347, 2004b).