

“Anticipatory Risk and Crisis Management Systems: Conceptual Issues derived from Historical Experience”

Professor Gordon Boyce
Dr. Paul Barnes
Queensland University of Technology

Abstract

What might the sinking of the Titanic and the 9/11 terrorist attack have in common? Although separated by 90 years, these two disastrous events stemmed from the failure of socio-technical systems to anticipate potential risks and provide an adequate crisis management response. All organizations are vulnerable as a result of pervasive uncertainty and the complexity of their underlying systems, and yet their leaders fail with alarming regularity to anticipate and plan for the unexpected. In many instances where cataclysmic breakdowns occurred, warning signs were detected but not responded to. History abounds with major organizational-technical disasters –the Tay Bridge, Titanic, the ‘flu pandemic of 1918-20, the R101 crash, the collapse of the Royal Mail Group, the Challenger explosion, Enron, and 9/11- yet planners have learned too little from the past. This behaviour is all the more curious because disasters occur frequently, some would say regularly, and others would go further to say that major failures should be expected.

This paper outlines conceptual issues derived from historical examples of major systemic failure, successful crisis management, and prevention. These instances of disaster and near-disaster reveal the importance of inflexible pre-set agendas, cognitive frames, communication channel design, hubris/organizational culture, and learning activities in enabling business and political leaders to anticipate and plan for major failure.

Introduction:

Failure in human systems within the public and private sectors are not unfamiliar events in the modern world with some commentators suggesting that such 'disturbances' may be increasing in complexity and in consequences (Lagadec & Michel-Kerjan, 2004).

Incidents that may on the surface seem purely technical failures have, after detailed causal analysis, been shown to exhibit more complex social and cultural elements. History provides an extensive retrospective of both recent and more distant organisational failures and disasters. Some incidents, such as the Tay Bridge collapse, have been shown to involve more than just elements of incomplete engineering design and construction but economic factors also. A number of aspects of mid-Victorian industrial life have been suggested as major causes of the bridge collapse: a bridge building frenzy, linked to the progressive and rapid expansion of railway construction, as well as commercial competition (Pinsdorf, 1997). Mileham (1998), more bluntly, suggests that the bridge was built with only two things in mind - speed of construction and cost.

It may also be correct to think of organisational failures as subsidiary to broader class of socio-technical crises. While the Tay Bridge collapse is obviously an industrial disaster, it emerges from a convergence of the social and technological advances of the time and, the economic development in post-industrialising Scotland. Further, while it is an important landmark in respect to changing the way bridges were designed and constructed (Lewis & Reynolds, 2002); the collapse remains relatively uncomplicated in comparison to the breadth and depth of consequences resulting from large-scale crises in recent times.

Analyses of major technical accidents over a number of decades concluded that approximately 20 to 30% of the causes of accidents sampled were technical in nature with 70 to 80% involving social, administrative or managerial factors (Turner, 1994). Social, administrative or managerial solutions were highly represented in the solution mix for these incidents. Given that the nature of most organisations entail humans and technology embedded together, it is logical to think of organisational failures in both the private and public sectors as elements within this broader class of socio-technical crisis.

Questions of critical importance to both the public and private sector relate to whether the learning derived from participation in such failures can actually reduce the likelihood of future failure or at least attenuate consequent impacts. With the presumption that causal and conditional evidence about such failures always awaits discovery and that humans and human systems do 'learn' from such events, the viability of anticipating future failure is self-evident. While such practices seem part of 'good business' it has been suggested that in the longer term, as operating circumstances change, organisations must also un-learn established practices (retain a capacity to adapt) in order to survive (Nystrom & Starbuck, 1984:53).

Establishing such an evolutionary capacity in organisations, however, requires more than the presence of strong and well-resourced internal control mechanisms derived from integrated corporate governance and risk management processes. The achievement of the dual outcome of learning and responsive control requires an openness and sensitivity to organisational vulnerability and adjustments to entrained ideas and practices that are likely to be outside prevailing corporate - managerial 'comfort zones.' While

transparency is a well-known aspect of corporate governance, regular and comprehensive assessment of institutional vulnerability may not be.

This work details a comparative examination of two iconic disasters (albeit separated by 90 years of social, technical and industrial progress) - loss of the Titanic and the September the 11th terrorist attack in New York. Both disasters will be examined within a common frame that spans the notion of socio-technical causality. The analysis is divided into four elements:

- *Meta-systems*: Contextual aspects of the wider national and trans-national settings relevant to the disaster;
- *Strategic Sense-making*: The gestalt of awareness and events influencing understanding of the incident and thus public sentiment and official perspectives¹
- *Tactical systems*: Higher-level aspects of decision making relevant to pre-incident settings;
- *Operating systems*: Aspects of the incident and response phases;
- *Post-incident Learning*: What did public, private and the lay communities learn from the event.

Each incident is examined in turn with a discussion on convergent and divergent issues following.

The Titanic Disaster:

The sinking of Titanic illustrates vulnerabilities stemming from weaknesses in the links connecting systems and sub-systems, as well as deficiencies in the systems themselves (see figure 1). The sad episode also highlights how mass media can be used to heighten expectations and misinform with the result that the consequences of a failure may be unnecessarily magnified. Public transmissions also unwittingly provided a cognitive framework for viewing the subsequent disaster from a highly adverse perspective.

Meta-systems:

At the level of meta-systems, that is those systems installed by statutory authorities, serious weaknesses were apparent. First, the Board of Trade rules governing ship construction had been formulated in the 1890s, and they had simply not kept pace with the increasing size of ships. For example, the rules compelled ships over 10,000 tons to carry a specific number of lifeboats, irrespective of how many persons the ship would convey. Nor was there any requirement for passenger lines to assign boat stations to each person or to conduct boat drills. Second, rules governing the height of bulkheads and double bottoms had not been revised in light of increased vessel size. Third, not all passenger ships had to be fitted with radios, and they did not specify that radios should be operated 24 hours a day. Fourth, established shipping routes allocated fairly northerly courses for vessels during winter, and there was no facility for monitoring ice conditions in the Atlantic. Under normal circumstances, the latter conditions would not have posed problems, but the authorities failed to allow for unusual climatic conditions like those that

¹ See in particular Weick, K.E. (1988) Enacted Sensemaking in Crisis Situations, *Jnl of Mgt Studies*, 27(4).

prevailed in the spring of 1912. Overall, the Board of Trade had allowed regulations to become obsolete.

Strategic sense making:

In terms of the highest organisational level, that representing strategic systems, management allowed public expectations to be raised beyond the bounds of prudence so that any mishap would critically impair corporate and personal reputations. Thus, the White Star Line sought to ensure that the construction and launches of Olympic in 1910 and her younger and larger sister ship Titanic (1911), were given maximum publicity in order to advertise the uniquely high standards of comfort (and safety) upon which the firm's competitive strategy was based. (In contrast, Cunard, White Star's main rival on the North Atlantic route, had gained significant advantages by adopting high speed as the distinguishing attribute of its two premier liners, Lusitania and Mauritania which entered service in 1906-7.) Technical journals and popular publications emphasized the amenities and the enormity (and by implication the safety) of the White Star ships. Indeed, after the Shipbuilder described Titanic as "practically unsinkable" the qualifier was omitted in subsequent articles in other publications with the result that the ship entered the public imagination as an invincible construct. Moreover, erroneous public statements made by the future master of Titanic, Captain Edward Smith, to the effect that he had never had a serious mishap in his 44 year career and that "modern shipbuilding had gone beyond all that" [i.e. design and construction had in essence overcome any peril of the sea] conveyed the same impression and returned to haunt White Star officials along with the ghosts of lost passengers.

Tactical systems:

At the next systemic level, design, several weaknesses would prove to be important. First, the bulkheads proceeded ten feet above the water line, so that when water filled a compartment it would soon spill into an adjoining compartment. In contrast, the Great Eastern built in 18XX but in many ways far ahead of its time in terms of design, had bulkheads reaching thirty feet above the waterline. Second, the cellular double bottom reached only six feet up the sides of the ship; in contrast the fast Cunarders had complete longitudinal bulkheads. Third, Titanic carried too few life boats to accommodate all passengers and crew. (Initially, Thomas Andrews's plans had included adequate lifeboat provision but on the orders of White Star's Chairman, J. Bruce Ismay, the number of boats was reduced to improve the view from the top deck.) Finally, access to the boat deck from steerage was poorly configured and the ship did not carry an alarm system. None of the vessel's design characteristics violated the Board of Trade rules, which as we have noted were out of date. However, the chief designer, Alexander Carlisle, did recognize the limitations of at least one regulation, but his recommendation was overruled on commercial grounds.

The links between middle level systems and those governing operations were also deficient. The first indication, chronologically, was the ship's trial. This lasted only 8 hours. Given the unprecedented size of the vessel, a longer trial was probably necessary to reveal more fully its handling properties. Indeed, when Titanic left Southampton harbour, the suction from its propeller caused a moored ship to break loose and a collision was prevented by a very narrow margin. (Earlier, sister ship Olympic had collided with a cruiser, HMS Hawke, when the latter was drawn into its side by the

suction created by the massive liner - both incidents suggest that skills needed to safely handle such large ships were deficient.) The second indication was the lack of any rigorous crew-training program. Titanic was put into service immediately after the completion of its trial, presumably management felt that seagoing staff could acquaint themselves with the vessel on the run from the builder's yard at Belfast to Southampton where it would embark the first group of passengers. To make matters worse, at Southampton the crew roster was revised, and *the first officer* along with other staff who had been on trip from Belfast were replaced. Thus, the continuity of acquired knowledge, limited though it was, was not preserved. Moreover, a "scratch" crew was put on board at the port of embarkation due to a coal strike that laid up other vessels. Staff were unfamiliar with the lay out of the ship – this would have serious consequences in the event that an evacuation became necessary, and team-based skills did not have time to develop among the crew, the officers, and between these two groups. Weaknesses in other links between the tactical systems and those governing operations became apparent later (see below).

Operating systems:

Turning to shipboard operating systems, a number of weaknesses were apparent. Proceeding from left to right along the bottom of the triangle in Figure 1, beginning with Safety, a boat drill was not conducted prior to the collision with the iceberg. Normally, White Star ships ran these drills every Sunday, but for unknown reasons this did not occur on April 14. When the collision occurred later that evening, crewmembers were not able to operate efficiently the boat lowering equipment, nor did they fill the boats quickly. In part this was because an accurate impression of the danger was not imparted to passengers, probably to prevent panic in light of the fact that the officers knew that the life boat capacity was inadequate. Moreover, the officers were afraid to load the boats fully before lowering them for fear that they would buckle under the weight; they had not been informed of the results of boat tests conducted at the builder's yard – these had shown that the boats could withstand the weight. Again, a vital link between the systems at the middle and lower levels were flawed. Overall, in the absence of an alarm system and assigned boat stations, evacuation procedures were chaotic. Stewards warned first class passengers by knocking on their cabin doors. Steerage passengers were constrained by locked gates and the need to find their way through unmarked labyrinthine passageways to find the boat deck. Many steerage passengers emerged into the well deck only to find that there was no direct access from there to the boat deck, revealing another design fault. From the captain, the officers and the crew, communication with the passengers was unclear and confused. Again, the aim may have been to prevent panic. Many of those crewmembers who joined the boats did not know how to handle them in the sea, reflecting the inadequacy of training processes. Nevertheless, some elements of the safety system worked well. The radio broadcast distress messages until shortly before the vessel sank, and the engineers stayed at their posts to sustain the electrical systems that powered the radio, the pumps, and the lights until nearly the end.

Next, the ship's communication system was afflicted by dual responsibility. Radio services were not run directly by White Star and laced under the authority of Captain Smith. Instead, the company sub-contracted with Marconi who provided the service. It was understood that non-fee earning navigation messages would be given priority over revenue generating private messages sent to or by passengers. (?) The structure of the contract created misaligned incentives. Indeed, on the fateful night Titanic's chief radio

operator told the California's operator to “shut up” when he attempted to send an ice warning because he was interrupting the private messages being sent to Cape Race. Not all navigation messages received by the radio cabin in Titanic reached the bridge as they should have; the most crucial message indicating that the ship was heading toward an ice field, which was much more dangerous than isolated bergs, was not delivered to the navigation officers. One other ice warning that was sent to the bridge was taken away by the Captain when he left the bridge. Prior to the collision, radio systems were subject to misaligned incentives and conducted in a haphazard fashion.

Aspects of Titanic's navigation systems were also run in deficiently. The vessel continued travelling at 22 knots even though the officers knew that they were entering an area where icebergs had been reported. Sensible precautions were taken, however, the look out was doubled and hatch doors closed to improve vision. Nevertheless, the lookouts did not have binoculars –these had been locked up by the first officer who left the ship in Southampton- and the officers on the bridge did not lend their glasses to the lookouts despite their repeated requests. When the lookouts sighted the iceberg at 11.40 pm, the first officer completely mishandled the steering with the result that the ship's side scraped the ice. In light of the configuration of the bulkheads and the double bottom, this was the worst eventuality possible. It meant that an opening occurred above the double bottom along six compartments with the result that the weight of water drew the ship down to where water slipped over the top of the bulkheads into compartments further astern. When informed of the extent of the damage, Thomas Andrews, Titanic's designer who was on board the ship during its maiden voyage, told Captain Smith that the ships would remain afloat for “1 hour possibly 2”. His assessment was a little pessimistic; Titanic foundered 2 hours and 40 minutes after striking the iceberg.

Analysis:

Thus, of the four operating systems analysed here, only engineering performed well, in fact beyond reasonable expectations. Navigation, communications, and safety showed serious deficiencies, and operating links between two critical systems, navigation and communications, were flawed. Defects in these horizontally aligned inter-systemic links were matched by weaknesses in the ties between vertically arranged systems. Vital information was not passed from construction and design to those in charge of the operating systems. The training and human resource functions that should have linked the two vertical system sets were utterly inadequate. Finally, the publicity generated by the strategic systems exposed the organization to a degree of public visibility that caused debilitating losses of goodwill when the unforeseen happened. (The fact that Ismay escaped alive when women and children perished undermined White Star's reputation further.) Indicating that public relations functions were appallingly deficient in general, White Star mishandled the ensuing crisis: Oswald Sanderson, a White Star Director, told a crowd outside the New York office that the ship was safe when he had no information whatsoever. In contrast, Cunard appeared in a highly favourable light. It was this firm's ship, Carpathia, which raced safely across nearly sixty miles of ice field in record time to rescue Titanic's survivors. Later investigation revealed that it was highly likely that California, owned by a White Star affiliate, ignored the rockets sent up by the stricken Titanic and did not activate its radio when its officers observed a ship operating erratically just a few miles distant.

Post-incident learning:

Two commissions, one in the US and the other in Britain, investigated the disaster. Senator conducted an inquiry that exposed the shortcomings of the White Star organization but did not succeed in finding sufficient negligence to justify legal prosecution. On the other side of the Atlantic, the Board of Trade conducted a tightly circumscribed investigation. The constrained character of the inquiry is not surprising because in effect the Board was investigating itself. Even though the investigation was essentially a white wash, new regulations emerged from it. The Board's new rules compelled all British registered ships to carry enough lifeboats to accommodate everyone on board. All ships carrying more than a set minimum number of passengers had to conduct 24-hour radio operations. Ship construction regulations were revised to improve internal subdivision, and masters in charge of ships running on the North Atlantic were instructed to adopt a more southerly course in winter. These provisions governed only British vessels; those of other nations were not bound to observe them. The United States government did not revise its maritime regulations after the disaster, but it did set up the Ice Patrol, the forerunner of the Coast Guard, to monitor ice conditions on the Atlantic.

9/11:

The success of September 11th attacks by al Qaeda on the United States is attributable to the careful planning of the terrorists and systemic deficiencies within America's law enforcement and defence arrangements. Indeed, the way in which the attack was organized strongly suggests that al Qaeda's intelligence unit had carefully analysed the structure of the US defence system and developed tactics to exploit systemic flaws. Catastrophic failure occurred at virtually every systemic level.

Meta-systems:

America's meta-systems were not aligned to prevent a terrorist attack. The law enforcement process was attuned to deliver justice not to compile evidence needed to understand and counter a terrorist attack. While individual government agencies did not share intelligence because lateral communication channels did not exist or were not used effectively (see below), in some critical instances legal and procedural guidelines deliberately constrained this type of transmission. Worse, incorrect interpretation of these regulations effectively prevented such exchanges. For example, the Foreign Intelligence Surveillance Act of 1978 required that approval for surveillance (like wire taps) had to be given by a separate court to ensure that this law could not be used to circumvent traditional criminal warrant requirements and vice versa. To protect human rights, the flow of intelligence information to the criminal branches came to be regulated through formal procedures laid down in 1995. The problem was that the rules were not understood and were not employed by those people who were supposed to use them. As a result, the procedures came to be referred to as "the wall" indicating that disclosures between the intelligence and criminal branches were seldom made. The Justice system was not, therefore, equipped to manage the interface between terrorist and criminal activities, while many terrorist groups, both foreign and domestic, used the proceeds from criminal activity to fund terrorist operations. (Nor was there the capability to cope with links between legitimate business and terrorism, even though the al Qaeda developed internal ties of this nature.)

The attack on the two US embassies in Kenya and Tanzania in 1998 compelled the US government to recognize al Qaeda as a serious threat to its interests. The near-simultaneous nature of the twin bombings at widely separated sites indicated that the terrorist group had considerable organizational capabilities. In response, The CIA developed a series of plans for kidnapping or killing Usama bin Ladin, striking his training camps in Afghanistan, and otherwise “attriting” al Qaeda’s capabilities. Most of these plans involved covert operations by the CIA working in tandem with the Northern Alliance or tribal groups in Afghanistan. Several reasons explain why none of these plans were conducted. First, the CIA’s reputation had been tarnished by earlier operations, especially “Contra-Gate”, which eroded public acceptance of covert activities in general and especially those that were of dubious legality or questionable morality. In this environment, the agency was hamstrung unless its operations were above question and targeted only proven terrorists. There was considerable difficulty proving that Usama bin Laden was guilty in a criminal sense as opposed to being simply implicated in anti-American terrorist activities. Second, these covert operations depended upon the co-operation of other governments and other interest groups. Here, the difficulty was that neither US diplomacy nor CIA activities succeeded in gaining the required consensus. Third, military operations –specifically in the most highly favoured form of launching cruise missiles against locations frequented by bin Laden- were frustrated by the lack of accurate intelligence. Without this crucial input, the US was unwilling to risk missile attacks that might cause civilian casualties; past incidents increased the amount of caution exercised on several occasions when some officials believed that they had bin Laden directly “in their sights”.

Strategic sense making:

At the strategic level, the security establishment was only beginning to make sense of the terrorist threat. Indeed, during the Cold War, the whole intelligence community had been focused on one particular type of *external* threat – attack by the Soviet Union. It did not fully grasp the nature of risks the nation faced when confronted by an international terrorist network supported by money and weapons from various sources and aided indirectly and directly by sovereign foreign powers. Previous attacks, such as the assault on the USS Cole and the embassy bombings in East Africa, had occurred upon US interests in foreign countries. Incidents of hijacking had most frequently occurred overseas and were designed to initiate negotiations for the release of terrorists held by foreign governments. The main exception to this pattern of behaviour was the bombing of a Pan American flight over Lockerby in the 1980s. There had not been a hijacking in the US for 30 years. The US uncovered a plan to hijack several American airliners and blow them up over the Pacific. The so-called Manila plot, envisioned simultaneous detonation intended to enhance the demonstration effect of al Qaeda’s capabilities. Moreover, the Oklahoma bombing focused attention toward domestic terrorists.

Nevertheless, by 1998, President Clinton had become concerned about the possibility of a terrorist attack on US soil by external groups using weapons of mass destruction, but here his fear was for a biological attack or a chemical attack of the type made by Aum Shinrikyo on the Tokyo subway system in 1995 (Report, 102). There were two precedents that might have directly drawn the attention of US authorities toward a threat to the homeland posed by foreign terrorists. The first was the bomb attack on the World Trade Centre in 1993. This was an assault directed toward a symbolic landmark, and it was intended to inflict mass civilian casualties. In this instance, the FBI’s investigation

was very effective and the legal system performed well, perhaps leading to overconfidence in existing organizational arrangements. At the same time, the amateurish mistakes made by one of the perpetrators Mohammed Salameh who repeatedly called the firm from which he had rented the truck used to carry the bomb in order to recover his deposit (he had reported the vehicle stolen) and was apprehended as a result, led US authorities and the public in general to underestimate the capabilities of foreign terrorist groups operating in the US. The second incident that should have forewarned US authorities about the threat foreign terrorists posed to the US homeland was the Ressam attempt to enter America in order to bomb LAX in late 1999. Nevertheless, it should be noted that none of the incidents listed above, with the exception of the assault on the USS Cole, entailed a suicide attack.

Overall, America's systems were focused on the wrong kinds of threat. While those systems identified al Qaeda as a source of varied threats, they did not have the necessary capabilities and the required mindset to eliminate it in a pre-emptive way or to anticipate what bin Laden might do next. Finally, none of the individual terrorist assaults that had occurred in the past provided a clear precedent for the 9/11 attack. However, careful analysis of all previous terrorist assaults at home and abroad might just have enabled officials to isolate individual elements from these incidents and combine them to anticipate the form of the September plan of bin Laden. Combining the suicide aspect of the USS Cole attack, with multiple hijackings like the Manila plot and the mass casualty aim of the World Trade bombing of 1993 would have advanced official thinking quite close to the form of the 9/11 assault. Following another line of thinking, running from terrorists using trucks to conduct suicide bombings, the common tactic employed in the middle-east, to using a boat as in the attack on the Cole, to using an airplane to mount a suicide bombing, might have suggested forms of possible threats. With a glimpse of these possibilities, the American government could have then assessed the responsive capabilities of its various agencies and then taken steps to improve them.

Tactical systems:

Had such an examination taken place, it would have discovered that intelligence gathering activities were conducted by a series of agencies, including the CIA, the FBI, the FAA, INS, and DEA, but the information was not shared or collated in a comprehensive manner (Commission Report, 78-84). Each agency operated like a silo and formulated its own local view of threats. What the US government lacked was a unit that could collate and analyse intelligence from all sources in order to develop an on-going appreciation of the situation regarding external terrorist groups. These basic functions, along with consideration of the forms of possible threats as suggested above, represent some of the first steps toward developing anticipatory capabilities.

In most cases, the threats identified by these agencies had nothing to do with foreign terrorists. The Immigration and Naturalisation Service (INS) was preoccupied with preventing illegal entry from Mexico even though the US was more vulnerable to terrorists coming via Canada, whose immigration regulations were far from stringent. Remarkably, border guards did not know that the immigration "watch lists" included terrorist suspects (Report, 81). The FBI field offices focused primarily on gangs, drugs offences, and other serious criminal activities. The Treasury Department, which controlled the Secret Service, Customs, and the Bureau of Alcohol, Tobacco and Firearms, was "not seriously enlisted for counter-terrorism" (Report, p. 82). Ironically, in

December 1999, an alert customs officer detained Ahmed Ressam as he tried to enter Washington State from Vancouver in order to bomb LAX [Report, 176-9].) The FAA also had an intelligence unit but it focused on convention hijacking and bomb threats, not suicide hijackers. This unit was linked to the FBI and the CIA, but in critical instances information exchanges did not take place. Thus, the FBI's assessment of flight training by terrorists and a definite warning of radical middle easterners undertaking pilot instruction was not passed to the FAA (Report, 83). On the eve of the September attack, only one part of the FBI and a separate unit within the CIA were engaged in counter-terrorism.

During the years immediately preceding the attack, several government departments attempted to strengthen their individual intelligence gathering capabilities in order to develop anticipatory capacity. For example, in 1998, in response to the attacks on embassies in East Africa, the FBI developed a five year plan to bolster national and economic security, but a lack of resources frustrated its implementation (Report, 76-7). The following year, the Bureau created a new counter-terrorism division that articulated a five-year plan, called MAXCAP 05, explicitly to build anticipatory capabilities. In the event, the FBI lacked the analysts, linguists, or technically trained experts needed to make any meaningful progress toward this objective.

Similarly, the CIA had made large long-term investments in intelligence analysing capabilities during the Cold War, but as the Soviet threat receded budget cuts eroded them considerably. When it attempted to build up its anti-terrorist capabilities following the embassy attacks of 1998, it was hampered by inadequate budget allocations (Report, 184-5). Nevertheless, the CIA did take a decisive step by setting up a virtual station, modelled on units that monitored a specific country, to focus on a single person – bin Laden himself. The unit was to devote particular attention to studying al Qaeda's financial structures and processes, but it lacked the skilled operatives needed to do so effectively. While the bin Laden station did accumulate considerable information about al Qaeda, it did not assemble such data in a comprehensive way and transmit it to the rest of the government (Report, 118). Quite simply, it had difficulty in convincing officials of its importance and managing information upwards. It was this same unit that devised plans for attacking Usama bin Laden and his organization, but as we have seen the operations it recommended were not executed, providing further indication of the CIA's inability to make its points heard and acted upon. Only the Head of the National Security Council's Counter-terrorism Security Group, Richard Clarke, was fully alert to the possibility of a bin Laden backed assault on the US mainland, but his repeated warnings diminished his credibility and caused chief decision-makers to downplay his assessment of the situation.

Overall, US intelligence gathering activities were widely distributed and ineffectively coordinated. Most agencies focused on threats other than those posed by foreign terrorists operating in the United States. Efforts to enhance intelligence and operating capabilities were frustrated, and what proved to be accurate assessments of the nature of possible threats were unappreciated.

Operating systems:

The September 11 attack directly affected three critical operating systems and the links between them. First, airport security arrangements provided a layered defence designed to catch hijackers even if one or more of the one of its four elements was breached. The

Computer Assisted Passenger Pre-screening System (CAPPS), based on the intelligence-derived “watch list” was designed to identify passenger who posed a threat. Airline ticketing officials identified such individuals and the principal measure taken usually was to delay the loading of their baggage until after their boarding of the aircraft had been confirmed. Identification by CAPPS did not result in passengers being subjected to any other security measures such as additional screening of body searches. The threat that this arrangement was designed to thwart was a bomb; the possibility of a suicide bomber or hijacker was not anticipated. The next layer was provided by airline agents who handled check in; they were supposed to identify passengers who behave out of the ordinary. The third element consisted of hand luggage screening, metal detectors and hand wand. Finally, on board security arrangements were intended to prevent hijackers from gaining access to the cockpit. Several of the hijackers were pulled up by one or more of the first three layers but were allowed to board their planes. In every case, they breeched on board security and entered the flight deck. On three flights, the hijackers, all of whom were seated in first class so as to be close to the cockpit, took control of the planes shortly after the fasten seat belt sign was extinguished. On UA 93, the assault occurred a little later. On all four flights, the hijackers subdued passengers by saying they had bombs on board. The inference was that these were “traditional” hijackings that would be resolved once the planes had landed and demands had been met. Only on UA 93 did the passengers see through this ruse.

The second system consisted of the FAA’s flight control operations. To direct flights, the FAA used 22 control centres grouped under regional offices that reported to a central command centre. The protocol laid down for hijackings assumed that the pilot affected would signal his flight controller by keying 7500 through his plane’s transponder. The controller who would be located at one of the control centres would inform his regional office which would then alert the central command centre. There a hijack co-ordinator would take over and inform the National Military Command Centre associated with NORAD. The NMCC would scramble a fighter to shadow the aircraft. These arrangements were based on the assumption that a hijacked plane would be readily identified through the transponder signal, that there would be time to pass information up through the channels to NORAD, and that any hijack would be of the traditional form.

In the event, the hijackers immobilized the transponders so that the planes disappeared from the air controllers’ screens. The FAA’s central command centre *did not* alert the NMCC; instead the Boston regional centre did so directly outside of the normal protocol. Fighters were scrambled but vectored into positions where they could not shadow or if needs be intercept the hijacked planes. The FAA’s central command centre did not inform all regional centres of the first hijacking so they could inform pilots on other flights to take additional security precautions until after the second plane struck the World Trade Centre. FAA officials were not sure whether it was their responsibility or that of the airlines to do so. Finally, the FAA’s central command centre ordered all planes in US airspace to land as quickly as possible. This directive was completely outside of the protocols.

The third system, NORAD, was not oriented toward asymmetric threats arising from within the United States. It was set up to deal with intrusions from outside US airspace, particularly by Soviet bombers. In September 2000, its existing plans anticipated that any order to shoot down a civilian plane would come from the National Command Authority,

which is from the President, the Vice-President, or the Secretary of Defence. Further, the plans assumed that any threat of this kind would originate from outside the US.

On September 11, these arrangements broke down. Command and control between the White House, NMCC and FAA was confused and afflicted by poor communication. The Vice-President did give the order to shoot down the airplanes but the NMCC did not absorb the information and it was not relayed to the fighter pilots who had been launched from Otis and Langley airbases. In the event, these fighters were hopelessly out of position to intercept the passenger planes. Acting completely outside of any protocol, the Secret Service ordered the scrambling of additional fighters from Andrews Air Force base.

In the face of an unforeseen threat – a multiple suicide hijacking- every one of the three operating systems malfunctioned. Moreover, the links between them broke down. Only the passengers on UA 93 prevented a successful suicide strike on a landmark.

Analysis:

America's vulnerability to the 9/11 attack arose from meta-systems that were not attuned to cope. These systems were based on rules of a game that was not played by terrorists. US officials were slow to make strategic sense of the threat posed by bin Laden. Richard Clarke's warnings were unheeded. The defence community was focused on threats of a traditional nature: Soviet attack and assaults on US interests abroad. The nation's tactical systems had developed splintered intelligence gathering capabilities and inadequate intelligence analysing capacities some of which had been eroded by budget cuts. Communication channels between the various agencies engaged in intelligence activities were ineffective. What the US lacked was a central unit that could collect and synthesise intelligence data. All three operating systems affected by the attack exhibited flaws and on the day of the assault none of them operated effectively and the links between them broke down. It is difficult to avoid the conclusion that the tragedy stemmed from complete systemic failure in US defence arrangements.

Post-incident learning:

Following 9/11 the US set up the Department of Homeland Security to exert unified control over intelligence activities, co-ordinate communications between all levels of government and develop crisis response capabilities. It consisted initially of four divisions: Transport & Border Security, Emergency Preparedness & Response, Chemical, Biological, Radiological, and Nuclear Countermeasures, and Information Analysis and Infrastructure Protection (www.dhs.gov President Bush June 2002). It was reorganized in November 2002 and now consists of the units listed above along with a science and technology development section, a Policy unit, and an operations unit. It is linked to the Chief of Staff and the military (www.dhs.gov. Reorganisation Plan 25 November 2002 and Organization Chart 11 July 2005). Operating systems have been revised comprehensively. Most noticeable are the more invasive arrangements for air travel security. In addition, sweeping changes in the legal system have been introduced.

While America's defence systems have been restructured to remove many of the defects identifies above, it is still a long way from building the international consensus needed to combat global terrorism. Some of its actions since 9/11 have raised questions about

human rights, especially those of detainees, and about the unilateral application of power. The nation needs to devote considerable energy to realigning its cognitive systems and those of other groups and governments upon which it depends for support.

Discussion:

Certain common issues are noticeable across the case studies examined. These are listed in Table 1 against the analytical schema referred to earlier. Critical factors in both events entailed failures of foresight and institutional capacities to respond to known signs of threat.

Table 1: Comparative Factors

<i>Analytical Schema</i>	Titanic	9/11
Meta-strategic	<ul style="list-style-type: none"> ◦ Trading and Commercial Shipping practice & policy 	<ul style="list-style-type: none"> ◦ Legal systems focused on judicial process ◦ Reactive national security stance ◦ Suspicion between Govt Agencies
Strategic	<ul style="list-style-type: none"> ◦ Commercial Imperatives ◦ Perceptions of Invulnerability 	<ul style="list-style-type: none"> ◦ Focus on the wrong threats ◦ Complacency
Tactical	<ul style="list-style-type: none"> ◦ Safety Design & Practices not followed 	<ul style="list-style-type: none"> ◦ Silo mentality – sharing intell. ◦ Intense & Wasteful redundancy of effort
Operating	<ul style="list-style-type: none"> ◦ Minimal pre-incident attention to safety and emergency response ◦ Existing safety systems not applied 	<ul style="list-style-type: none"> ◦ Prevention systems hardwired to expected set of scenarios ◦ Communication & coordination failures
Common Patterns	<ul style="list-style-type: none"> ◦ Flaws in individual mitigation systems ◦ Horizontal control links between operational systems ◦ Weakness in vertical links between operational, strategic and meta-systems (Impacting decision-making and Governance). ◦ Limited nature of post-incident learning. ◦ Weak ties in networks and the “outsiders” 	

It is suggested that in both case studies there is little evidence of capacities to *anticipate* and mitigate risk (i.e. the likelihood of loss- causing incidents). Effective risk management generally includes examination of higher order contingency planning activities derived from steps that:

- Recognize the presence of external and internal threats;
- Define both the likelihood and consequence of potential incidents (based on a thorough understanding of threat environment and the vulnerabilities within institutions (and other societal factors);

- Consider how threats might, via an existing vulnerability, increase the likelihood of harm or loss;
- Scan for signs of the emergence of referent threats and maintain a capacity to respond once noted;
- Ensure that adequate capacity and capability exists within and across institutions in order to deal with emergent harm-causing incidents (under crisis conditions).

Given these steps, it is presupposed that an organisation has completed (and frequently re-assesses) comprehensive vulnerability analyses; that is, it must target processes and capabilities critical to normal and planned functioning. It is also assumed that the *anticipatory* capacity is represented by multi-disciplined teams, the members of which are expected to think ‘outside the square’ with respect to recognizing intelligence data (often seemingly unconnected) that indicate signs of a plausible threat – based on a knowledge of how ‘things’ currently operate; or probable threat – derived from what is likely to happen given the continuance of existing trends (after Voros, 2003).

A final expectation is that when the formalized anticipatory system is triggered, a decision-support process ensures that, if needed, resources are allocated so as to apply the incoming intelligence in an intelligent way.

Issues for Further Development:

The notion that applied historical analysis: using a back casting (retroactive analysis and pattern identification) and forecasting (seeking to map likely scenarios) deserves further effort especially in relation to institutional continuity and national security outcomes.

Confirmation of valid methodologies that support both back and forecasting in a regularised and grounded manner would extend this work. While existing approaches are helpful, efforts to confirm their ongoing applicability - given the changing nature of the world and socio-technical activities human – are needed.

References:

Lagadec, P. and Michel-Kerjan, E. (2004) "Meeting the Challenge of Interdependent Critical Networks under threat: The Paris Initiative, Anthrax and Beyond," Cahier No. 2004-014, Laboratoire D'Econometrie, Ecole Polytechnique, Paris.

Lewis, P.R. and Reynolds, K. (2002). Forensic Engineering: A Reappraisal of the Tay Bridge Disaster. *Interdisciplinary Science Reviews*, 27(4), pp. 287-298.

Mileham, G. (1998) *The Tay Railway Bridge*
<http://web.archive.org/web/20020609121056/http://www.brad.ac.uk/acad/civeng/marketng/civeng/failtay1.htm> accessed 17/02/2005 2:04 PM,

Nystrom, P.C. and Starbuck, W.H. (1984). To Avoid Organisational Crises, *Unlearn. Organisational Dynamics*, 12(4), pp. 53-65.

Pinsdorf, M.K. (1997). Engineering into Disaster: History of the Tay Bridge. *Business and Economic History*, 26 (2), pp. 491-504.

Turner, B.A. and Pidgeon, N. (1997). *Man-made Disasters* (2nd edn), Butter-worth Heineman, Oxford.

Voros, J. (2003) 'A generic foresight process framework', *Foresight*, Vol. 5, No.3, pp.10-21

Case Study Bibliography:

Boyce, G. (1997) "Business implications of the Titanic disaster", Public Lecture Series, Wellington Maritime Museum, 1997

National Commission on Terrorist Attacks Upon the United States (2004) *The 9-11 Commission Report*, Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition.