

QUT Digital Repository:
<http://eprints.qut.edu.au/>



Barnes, Paul H. and Charles, Michael B. and Branagan, Mark A. and Knight, Alistair (2007) Intelligence and Anticipation: Issues in Security, Risk and Crisis Management. *International Journal of Risk Assessment & Management* 7(8):pp. 1209-1223.

© Copyright 2007 Inderscience

Intelligence and Anticipation:
Issues in Security, Risk and Crisis Management

Paul Barnes*, Mark Branagan, Michael Charles, Alistair Knight

***Corresponding Author**

School of Management,
Faculty of Business
Queensland university of Technology
Brisbane, Australia
GPO Box 2434,
Brisbane Qld. 4001.
Australia.
Tel. +61- (0)7-3864-9019
Fax. +61-(0)7-3864-1771
E-mail: p.barnes@qut.edu.au

Paul Barnes teaches risk and crisis management in the School of Management, Queensland University of Technology. He has undergraduate qualifications in Environmental Science and a Doctoral qualification in Risk Management and Organisational Analysis. Previous experience includes holding the positions of Corporate Risk Manager, Queensland State Department of Primary Industries and Manager of the State Public Safety Unit of the Queensland Fire and Rescue Service. Before coming to the Faculty of Business School he was Director of Security Policy Development with the Defence Security Authority, Australian Department of Defence, Canberra, Australia..

Mark Branagan is presently a PhD candidate at the Information Security Institute, Queensland University of Technology. His research includes risk management and assessment for Critical Infrastructures especially Information Infrastructures, development of simulation frameworks for risk in complex systems and information security issues raised in complex Information Infrastructures.

Michael Charles is a Research Fellow in the School of Management, Queensland University of Technology, Brisbane, Australia. He has a Master of International Business Studies, in addition to a PhD in Ancient History from the University of Queensland. He has taught ancient history and historiography, published on aspects of military history. In addition to these interests, his current research areas include strategic management, public administration and economic history and risk and crisis management.

Alistair Knight is a serving officer in the Royal Australian Air Force. He holds a BSc from the Australian Defence Force Academy and the University of New South Wales.

Intelligence and Anticipation:

Issues in Security, Risk and Crisis Management

Abstract:

This article deals with the way in which intelligence flows and other critical information can be embedded into a risk framework that will facilitate the early warning of emerging threat scenarios. That is, an organization should be able to *anticipate* crisis triggers and know when a crisis situation will manifest. As an outcome, a conceptual framework that defines how to make sense of complex situations, data sets and real world anomalies is suggested.

Keywords: Threat Assessment, Intelligence, Sensemaking, Anticipation, Vulnerability.

1.0 Introduction

Recent events have revealed that the intelligence systems of today's organizations, be they government, private-sector or military, are too rigid and steeped in routine to adapt to the growing (amount) number of variables and informational sources that are available.¹ This being the case, today's organizations are faced with the possibility of having a valuable and potentially threat-averting datum enter their organization, only to have that particular datum not accorded the attention that it should warrant. This work will deal with expanding the sensitivity to the broader threat context or, in other words, increasing the range and scope of an organization's threat assessment capacities. A concomitant of this is that more diverse and non-traditional intelligence sources will need to be factored into intelligence gathering activities so that a more accurate appreciation of the threat environment can ensue. Once this expanded threat context is established, and after the new parameters have been embedded into the intelligence system, the organization will need to increase its sensemaking² capabilities in order to gain the maximum value from the newly 'regularized' conduits of intelligence.

The capacity of an organization to recognize threats (as sources of potential harm or loss) is critical. The likelihood that such threats will manifest themselves as a loss-causing incident

will be dependent upon a number of factors, with vulnerability of the organization or its systems to a threat – or a set of threats – being of paramount importance. From this perspective, the paper seeks to posit the means by which a greater symmetric fit can be promoted between a range of threats (once identified), and the ability of an organization to recognize and respond to them.

The work begins with an examination of formal and informal means of intelligence acquisition by organizations. It then provides a historical example from the Pacific theatre of World War II that emphasizes a failure to pay attention to a relevant, timely and – in retrospect – critical intelligence flow concerning the capability of the Japanese Zero fighter plane that was received well before the opening of hostilities between Japan and the Allies in December 1941. Following this, we examine specific cultural vulnerability factors within organizations that can exacerbate pre-existing inadequacies in intelligence gathering and analysis capacity. The paper concludes with a discussion of a conceptual framework that embeds aspects of threat, risk and crisis management into a coordinated organizational capacity that supports the anticipation of emergent threats and supports effective crisis responses.

2.0 A Symmetric And Asymmetric Dichotomy

Organizations in our increasingly complex world need to be equipped with the ability to ‘make sense’ of critical aspects of the information that filters through to them. This information or data may be available from diverse sources and may be transmitted by various means. For the sake of argument, it is expedient to narrow these means down to two broad rubrics, these being (a) *Formal* (i.e. organizationally embedded intelligence conduits) and (b) *Informal* (i.e. non-organizationally embedded intelligence conduits).

Thus intelligence may arrive in a formal fashion, such as by means of a dedicated intelligence division or regularized authorities, correspondents and consultants; or it may arrive in an informal fashion, i.e. by a means or conduit not effectively ‘plugged into’ the relevant decision-making systems or units of the organization. Thus we might suppose that information arriving through an established and formalized route is generally given greater importance (and indeed credence) than information that arrives as a result of other activities, or by mere happenstance. Indeed, we might infer that information actively sought by the

organization is given greater priority in comparison to what might well be termed informal data.

In short, having arrived in a formalized and prescribed fashion according to established procedure; the datum can be processed – all things being equal – in an appropriate fashion. This process is facilitated by the intelligence procedures and protocols already in place. What this effectively means is that information collected via the formal intelligence gathering system already embedded into the organization is fed into the formal decision-making system of the same organization. In this paper, we will assume that organizations have the ability to deal with formally sourced data, especially since a symmetric fit should already exist between an identified threat and the ability of the organization to recognize it and respond to it.

Problems, however, occur when information enters the organization in an informal way, i.e. by means of a conduit that, as we have said, is not effectively ‘plugged’ into the organization’s existing analytical and decision-making framework. In such circumstances, the value and import of the intelligence datum, we might posit once again, is not accorded the priority that it might warrant if it had entered via a more formal conduit. What is more, the datum may not correlate with threat scenarios that have been identified by the decision-making or intelligence personnel within the organization. In short, there exists an asymmetric fit between the threat and the ability of the organization to recognize it. If the datum cannot be positioned directly in the existing threat context, it may well be dismissed as unimportant. In an even more unfortunate train of events, a datum that could be of great relevance to the organization is either discarded as irrelevant, filed away, directed elsewhere, or completely ignored. Worse still is that these activities are often prosecuted by an employee or agent of the organization who is not equipped to make the appropriate decision regarding the datum’s utility value or otherwise.

3.0 Intelligence Symmetry & Asymmetry in History: The Case of the Zero Fighter Plane

The threats that command most of our attention at the present time may not represent the most salient concerns of the future. Indeed, an absence of forecasting capacities at an organizational level serves to increase vulnerability (as a predisposing causal factor that increases the potential for error), and decrease the ability of the organization to deal with

hitherto unforeseen threats once they are formed. To put this concept into context (and concomitantly demonstrate the way in which the formal and informal reception of intelligence information affects the treatment of an intelligence datum), we might well look at a classic example of the way in which a seemingly important intelligence datum was not acted upon. This is necessary in order to demonstrate that threat scenarios, which appear so obvious with the benefit of hindsight, may not be recognized by an organization in real time. In the following case study, failure to act upon such an intelligence datum, which entered the organization via informal means, resulted in greater harm to the organization than might otherwise have been the case had it been acted upon in the appropriate fashion.

The Mitsubishi A6M Zero-Sen naval fighter (codenamed ‘Zeke’ by the Americans) won renown as the scourge of Allied aircraft in the early stages of the Pacific War. Though its capabilities and performance have often been exaggerated (perhaps in order to disguise what might be perceived as the dismal failure of Allied intelligence with respect to anticipating and responding to the threat), it nevertheless caused a tremendous surprise to the Allies (Franks, 1986, 103). Moreover, until the arrival of more capable Allied naval aircraft, such as the Grumman F6F Hellcat and Vought F4U Corsair,³ the Zero achieved virtual air superiority wherever it operated. The Zero regularly outmanoeuvred the Hawker Hurricane, one of the heroes of the Battle of Britain (Cull and Sortehaug, 2004, 36).

The Zero, as it came to be called by friend and foe alike, presented a highly unpleasant surprise to the Allies from Pearl Harbour (7 December 1941) onwards. Yet this particular aircraft had been operational since July 1940, when fifteen pre-production A6M2s were sent to China for the purpose of combat trials with the 12th Rengo Kokutai (Mondey, 1996, 194; Francillon, 1987, 365). These aircraft were soon withdrawn once they had demonstrated their complete superiority over the defending Chinese aircraft. At this time, the famed American Volunteer Group (AVG), christened the ‘Flying Tigers’ by the local Chinese, became aware of the Zero and its threatening capability. Their commander, Claire Chennault, a retired officer of the United States Army Air Corps whose abrasive and forthright demeanour had failed to enamour his more tactically conservative superiors,⁴ was so impressed and – presumably – concerned that he wrote a report to his former employer.

This report was delivered when Chennault visited the United States in the autumn of 1940. According to Chennault (1949, 93), he felt that, “as a retired Air Corps officer”, it was

his “responsibility [to pass] ... on to the American authorities any military information that was available”. In his report, he outlined the danger posed by these new and impressive aircraft, which, being lightly constructed and possessed of drop-tanks (not used by Allied aircraft, or those of the Germans, until later in the war), had extraordinary range and were highly manoeuvrable (Gunston 1980, 126). Technical information, such as could be ascertained, was also included.

Strangely enough, the report was ignored, which prompted Gunston (1980, 126) to suppose, somewhat humorously, that “his warning was obviously filed before being read”. As Chennault (1949, 94) himself later wrote, “Air Corps technical manuals on Japanese aircraft in use at the time of Pearl Harbour [7 December 1941] devoted a blank page to the Zero”. Jiro Horikoshi, the Zero’s chief designer, later reported with astonishment that, even after the Zero had been used in combat for a whole year, the monthly American aircraft magazine to which he subscribed “never carried a single line about the Zero” (Horikoshi, 1981, 107).⁵

Furthermore, “American pilots got their first information on its performance from the Zero’s 20-mm. cannon a year later over Oahu and the Philippines” (Chennault, 1949, 94). One might also note that Chennault’s dossier on the highly manoeuvrable Nakajima Ki-27 (codenamed “Nate”) of the Japanese Army, one example of which had even been captured and combat tested against three Western fighters in China, namely the Curtiss P-36, Gloster Gladiator and the Polikarpov I-16, also failed to influence the Allies (Chennault, 1949, 93; Samson, 1987, 60). The United States War Department sent a letter in order to thank Chennault for his efforts, with the promise that the data would be forwarded to “aeronautical experts”. But these “aeronautical experts” eventually declared that the aircraft described by Chennault could not be built (Schultz, 1987, 75). Indeed, it was discovered in 1940 that the file had gone missing – “The Air Corps had never even seen the dossier” (Chennault, 1949, 94).

As now seems clear, if the Zero pilot lured its generally bulkier adversaries down to lower altitudes and forced them to reduce speed, the Japanese aircraft held the advantage. But, if the fighting occurred at higher altitudes, Allied aircraft outclassed at lower altitudes (such as the Grumman F4F Wildcat) marginally had the upper hand (Franks, 1986, 113). It seems, therefore, that the Zero achieved air superiority in the initial stages of the Pacific War

largely because American and Allied airmen did not understand the aircraft's strength and limitations. As Franks (1986, 112) points out, "abysmal intelligence led Allied nations to believe that in 1941 Japanese aircraft were inferior copies of their own previous generation", a situation which was quite the reverse of the generally splendid intelligence-gathering that underpinned Japanese operations in the early stages of the Pacific War (Cross, 1987, 163). However, once the Americans and their allies learned that they should avoid low-speed dogfights at low-altitude, the Zero, which was in no way a technically sophisticated fighter by mid-1942, could be mastered by aircraft already in the possession of the Allies.

Put in terms of the notions detailed in this paper, Chennault's report had entered an organization whose threat assessment capacities were, at that time, inadequate for detecting the danger posed by Japanese air power, even though it must have been recognized at higher levels that conflict with Japan was more or less inevitable. Moreover, intelligence regarding the Zero had entered the organization in what we have described as an informal route; that is, it was (a) transmitted by a person with no formal ties to the organization (and who was foolishly regarded as something of a crackpot), and (b) was received and processed by members of the organization who were either ill-equipped to deal with this particular intelligence datum, or did not correlate it with known threats. The above is especially damnable since Chennault was made commander of the Fourteenth Air Force in China after his reinstatement in 1942, and eventually rose to the rank of major general (Schultz 1987, 236 and 290). Again, we see an instance of asymmetric fit between ineffective capacity and an existing threat environment.

With this historical example, it becomes obvious that even large organizations that might pride themselves on intelligence-gathering and intelligence-processing ability may not deal effectively with data that enter the organization in an informal fashion, especially if unsolicited. In short, if (a) the range of the United States War Department's threat assessment capacities had proved capable of identifying the threat posed by Japanese air power (and the existence of the Zero in particular), and (b) the datum regarding this had entered the organization via formal means rather than by means of unsolicited communication from somebody deemed to operate outside the organization, Allied pilots would have been alerted to the danger imposed by the highly manoeuvrable Zero in its favoured operating environment. Thus the threat could have been *anticipated*, and the Zero might not have appeared as invincible as it did in the desperate and testing first months of the Pacific War.

4.0. BEYOND SYMMETRY: Factors in Organizational Surprise

Surprise has always had an egalitarian affect in society. To be surprised in a pleasant fashion is preferable to the alternative. Unfortunately, the alternative state has, as shown above, been present more often than not in international conflicts and in many organizational crises through time. In light of the details discussed above, we need to devise the means by which the range of our threat recognition capacities can be enhanced so that threats and threat sources that presently sit beyond our conceptual horizons are brought more quickly into view. It stands to reason that we would benefit from being able to make sense of the nature of the threats. Indeed, if we are to anticipate emergent issues with greater promptness, and thereby minimize their impact or mitigate the likelihood of their manifestation, we need to look beyond existing embedded or ‘formal’ systems of searching for, receiving, prioritizing and acting upon intelligence data. According to the present line of thought, this should be able to be achieved by (a) regularizing the ‘informal’ conduits of organizational information reception so that such data can be brought into the view of decision-makers within the organization, and (b) by embedding this capability into a sustained structure.

The notion of ‘abysmal’ intelligence, in the case of the Zero, includes both issues of access and competencies to analyze data once available. In retrospect, the information existed in a relatively complete and accessible form (though a captured Zero was not yet available for flight-testing), but it was not acted upon as far as one can tell – it was not ‘bad’ information, rather it was a ‘bad’ use or rather *non-use* of *available* information. A deeper insight may be that, as a war-fighting entity, the United States, at that point in time, not only lacked pre-validated intelligence but also lacked a capacity for timely processing of intelligence and defining wider (prospective) intelligence-needs. Such failures are not limited to national security settings. Indeed, they are also relevant to corporate and institutional arenas.

The reader might wonder how such situations could come about. Perhaps the answer lies in the structural rigidity of intelligence facilities that often exist within established organizations. Holmberg (2001, 72) draws our attention to the fact that the “total knowledge space ... may be a space with many dimensions and a complex topology”. Holmberg (2001,

72) adds that this space might best be thought of as “four two dimensional fields”, these being:

- 1) What you do not know that you know (i.e. unconscious knowledge);
- 2) What you know that you know;
- 3) What you know that you do not know, and;
- 4) What you do not know that you do not know (i.e. a condition of ignorance).

It could be argued that any ‘self aware’ intelligence-seeking institution would be active in uncovering aspects of Field 1 and consolidating a capacity to leverage the benefits of Field 2. Equally important, yet often more difficult, are the challenges of Fields 3 and 4. Where the former requires objectivity, the latter requires intense honesty and critical institution-wide reflection. The influence of Field 4 factors also presupposes an interest in flexibility, exploration, and knowledge seeking across institutions.

In the context of what has been put forward, an intelligence datum that enters the organization may confront employees who may not be aware of what potential threats have not yet appeared on the radar, but are nevertheless lurking perilously close to the periphery. Once again, we must think of an asymmetric fit with existing organizational capacities. In a practical sense, this may mean that these threats cannot be anticipated because they are not yet known to exist. At the final extreme (which could be a state of ubiquitous ignorance), active denial of the existence of any unexplored threat might be common. In turn, the non-recognizance of impending threats, and their operational context, affects the way in which intelligence data are processed. If an intelligence datum enters the organization via formal means, there is still some chance that, even if it does not correlate with previously identified threats, it will still be used to anticipate or recognize an emerging threat (indeed, this datum might help expand the range of the organization’s threat assessment capacities). In the case of data entering by informal means, there is presumably an increase in the likelihood that an important intelligence datum pertaining to an emergent threat scenario will not be recognized or acted upon.

Analyses of recent iconic corporate and institutional failures and their aftermaths have shown that, in addition to pertinent causal triggers of crises being unexpected and predisposing factors being overlooked, the capacity to respond quickly and appropriately, once emergent signs are noted, often seems to be restricted. Specific organizational cultural patterns or ‘operating rules’ have been retrospectively linked to the genesis and amplification

of many well-known organizational crises. It has been strongly argued that the presence of such patterns in an operational repertoire increases vulnerability and the likelihood of accidents and crises (Perrow, 1984). Of the many patterns that have been examined (Smart and Vertinsky, 1977), two are pertinent to the fate of intelligence data once they enter an organization. These are as follows:

- ***Rigidities in Thinking:*** Restricted expectation about contingencies and their consequences, inflexibility in considering alternative options and choices for mitigation;
- ***Information Distortion:*** Attenuation and filtering of information to key decision-makers.

Information filtering can lead to a reduced organizational capacity in terms of making operationally difficult decisions. Over time, attenuation of information, especially if it relates to the functioning core of sub-systems, can lead to organizational blindness. Patterns such as this support the notion that failures ‘incubate’ and that an inability to recognize and respond to the presence of ‘warning signs’ is symptomatic of crisis-prone organizations (Turner and Pidgeon, 1997; Pearson and Mitroff, 1993; Mitroff and Alpaslan, 2003). Crises and their consequences might also be regarded as not only the result of a failure to notice signs, but also the result of a failure of organizational systems to respond to them.

Timely communication relevant to threat recognition and crisis mitigation can be filtered out, especially if ‘upper layers’ of management find the content inappropriate or unacceptable (Weir, 2004)⁶. Analysis of events leading to the loss of the space shuttle Columbia indicate that NASA officials initially rejected foam strike as the proximate cause of the accident and, as a matter of faith, held steadfastly to this belief – even in the face of accumulating evidence and strong interventions of in-house engineers. Studies report that rigidity in the erroneous belief held by some members of the managing hierarchy was such that requests to gather more evidence via satellite or telescopic imagery were denied (Mason, 2004).

Organizations such as NASA, or indeed any entities that develop and/or use advanced technology across a range of disciplines, do not always have detailed operational experience that constitute a basis of familiarity and learning (Marais *et al.*, 2004). Furthermore, experience with old technologies might not be applicable to newer ones. For example, digital systems such as fly-by-wire avionics or transnational information and communication

technology systems may paradoxically affect the frequency, nature and understandability of accidents. Marais *et al.* (2004) further suggest that advanced technical systems might change the type of errors made by operators and that older, electro-mechanical systems have little evolutionary link to new system designs and technology, which means that familiarity with older systems will not necessarily translate to familiarity with newer ones.

If such incomprehensibility factors are combined with an organizational culture that is crisis prone with heritable characteristics such as rigidity of core beliefs and values, assumptions of competency, ineffective communication and information sharing capacities, in addition to misplaced belief in its own expertise, the organization may be incapable of learning and generating flexible responses to crisis events (Smith, 1999). Referring again to recent snapshots of organizational culture in NASA, Mason (2004) suggests that the causal context of a failure may be deeply rooted in the organization's history. Despite this, the agency's long string of previous successes may have led its managers to believe that they could do no wrong. As can be seen, this attitude of omnipotence and omniscience is very dangerous when dealing with interactively complex, unruly and ultimately unpredictable technology (Mason, 2004).

Early warning and effective communication remain key factors in the literature and professional practice of crisis management (Wisnblit, 1989). As suggested earlier, faulty or untimely communication is implicated in the aftermath of many well-known organizational crises. The failure to notice signs in the pre-condition phase of a failure process is unlikely to be the result of inattention. Rather, it may be a compound issue of deficiencies in the communication mechanisms, and differences in functional worldviews between layers of an organizational hierarchy.

Issues such as those referred to above have been identified in post-'September 11' analyses and are specifically noted in the 9/11 Commission Report. The Report details, for example, that the FBI lacked a capability to link the collective knowledge of agents in the field to established national security priorities. The acting director of the FBI first learnt of his agency's hunt for two possible al-Qaeda operatives in the United States and the arrest of another Islamic extremist who was undergoing flight training on or about September 11. Furthermore, the Director of the Central Intelligence Agency knew about certain critical FBI investigations weeks before word of them made its way even to the FBI's own assistant

director for counterterrorism (National Commission on Terrorist Attacks Upon the United States, 2004, 352).

The importance of systemic complexity in explaining organizational failure has been noted extensively. Indeed complexity is also a key factor in threat analysis. The recognition of adequate managerial structures, in circumstances of complexity and uncertainty, is supported conceptually by the ‘Law of Requisite Variety’ (Ashby, 1986). Clearly stated, this aphorism suggests that the variety of a regulator (or control system) must equal that of the variety of the situation being regulated. Thus if an issue or problem is complex, any group deployed to analyze options and/or provide solutions must be able to exhibit an adequate variety in analytical repertoire in order to map the difficulty of the problem at hand.

As an organization’s complexity increases (in size and functional interdependency), so too must the sophistication and variety of the acquisition of corporate information and provision of regulatory control. While the need for comprehensive information in such circumstances is critical, it must also be timely and be couched in forms that *aid* decision-making rather than impede it. In addition, it should be borne in mind that there is no causal link between extra information and better decisions (Sarewitz and Pielke Jr., 2001). In fact, too much information or an influx of new data can detract from balanced decision-making or, in extreme cases, result in what military organizations call ‘command paralysis’. Full awareness of these organizational issues is central to creating useable knowledge as a decision-support aid in uncertain contexts (Sarewitz and Pielke Jr., 2001).

Learning *from* and *about* failure is a form of *Sensemaking* that, in retrospect, illuminates how decisions were implemented. The reaction of Sir Winston Churchill after the fall of Singapore in the Second World War is an interesting consideration. Allison (1993) notes that Churchill asked four rhetorical questions in his role as leader: “why didn’t I know?”, “why wasn’t I told?”, “why didn’t I ask?”, and “why didn’t I tell what I knew?” It is logical to assume that no one person could ask these questions and that, by extension, it would take organizational knowledge to answer them. From an organizational fitness perspective, appropriate ‘learning’ variations of the questions are: “how will I know?”, “how will I ensure that I am informed?”, “when should I ask?”, and “when should communication be triggered?” It may be that organizational learning starts with ensuring the presence of internal capacities to ask such questions in order to reduce the possibility of being surprised,

and then determining if organizational policies and functional systems support the effective and timely delivery of the answers.

5.0 ANTICIPATION: A Convergence of Analysis and Sensemaking

A common theme of this paper is that intelligence gathering entities must remain flexible and receptive to multiple sources of information. Some of this information will be unsolicited and most of it will be of unknown credibility or reliability. In a traditional sense, intelligence functionaries, be they government or private, collect information, analyse it, and develop a broad contextual picture of its implications. The accuracy and temporal relevance of this broad picture relies on an organization's collection capacity and the skill of its analysts. A key vulnerability of this system is that it becomes easy for analysts to believe that their *Weltanschauung* ('world view') is completely accurate. In view of this, the organization can develop the habit of rejecting any information that does not correspond with the prevailing worldview.

Let us apply this to the earlier example of the Zero. Since the analysts in the U.S. War Department held the worldview or picture that, in 1941, "Japanese aircraft were inferior copies of their own previous generation", unsolicited information that disputed this picture was rejected with obvious consequences. In essence, predicating all assessments on a predetermined *Weltanschauung* will make it impossible to protect adequately against threat sources of unknown or unexpected origin. That is, it will be impossible to deal adequately with what Holmberg (2001, 72) would call "What you do not know that you do not know".

We propose an alternate method for conducting intelligence assessment inspired by applied risk management philosophy. Rather than developing a *Weltanschauung* based on incomplete and sometimes inaccurate information, and then using this context to make predictive assessments with regard to emerging threats, we suggest that, as a first step, thought should be given to identifying critical organizational or institutional vulnerabilities. These vulnerabilities can then be used, as opposed to the predetermined reality construct, as the filter through which grains of relevant information can be sorted from the chaff.

Filtering vast quantities of data in order to discern a pattern may not be an optimal way to 'do intelligence' (Meyer, 2002). The ideal approach is to decide what might be happening with

respect to an issue or threat and then create the analytic process with a view to seeking signs that such an issue is active – or, conversely, is not active. Aligned to this approach is the need to know, in advance, what you would expect to see if the issue or threat were active. This notion is similar to hypothesis creation and testing, which constitutes part of scientific method, but entails greater options for variability than a null and alternative hypothesis. In short, this allows more opportunity to embrace descriptive ambiguity.

But there are limits to the amount of ambiguity and hypothetical frames that human analysts can address. Holmberg (2001) suggests that, compared to the total possibility of knowledge (including aspects of institutional vulnerability such as current and emergent threat sources), a single individual's knowledge quotient will be insignificant. However, the pooling of Field 2 Knowledge Space capacities (i.e. "what you know that you know") of many individuals and their subsequent application to an effective subset of relevant multiple hypotheses may help to overcome this limitation (Holmberg, 2001). This pooling effect is a manifestation of the requisite variety in both team development and in providing the team with a multiplicity of alternative options for consideration.

So, *Anticipation*, as a functional capacity to mitigate risk (i.e. the likelihood of loss-causing incidents), is enabled by a diversity of team-based skills and emergent insight. Anticipation, therefore, logically requires that the team be empowered and encouraged to make use of the emergent scanning capacities in order to consider the relevant knowledge base(s) and pursue multiple causal hypotheses. Such teams must also use a systematic framework to both guide their thinking and contextualize their findings and recommendations. It is suggested that specific practices derived from an application of risk management theory provides the basis for such guidance.

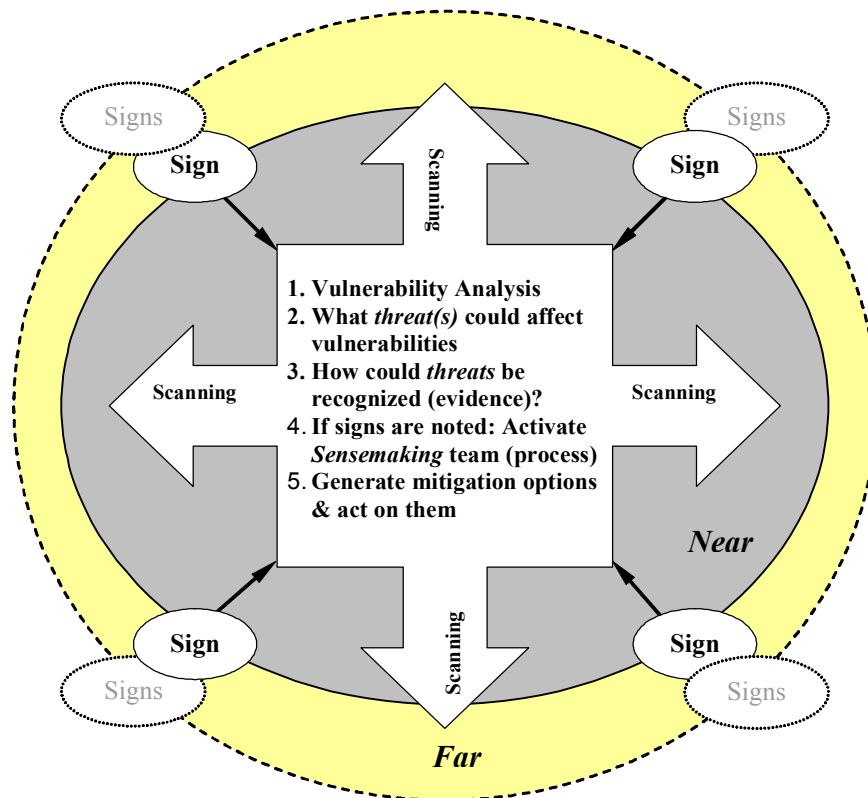
Effective risk management generally includes examination of higher order Continuity and Contingency Planning factors derived from proactive steps that:

- 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;
- Ensure that adequate capacity and capability exists within and across institutions in order to deal with emergent harm-causing incidents (under crisis conditions).

A fourth factor common to these three elements is the timely flow of information (i.e. processed intelligence) to key decision-makers. Thus, while the issue of symmetric and asymmetric access to intelligence is important, the wider implication of institutional governance, as it interfaces with security risk management and crisis response capabilities, emerges as ‘the other side of the coin’.

As a consequence, anticipation is an active *Sensemaking* process that requires the support of a mature and effective risk management capability embedded within an organization. Figure 1 describes aspects of how this process could operate.

Figure 1: **Anticipatory Sensemaking Framework**



In this framework, 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.

Once again, we might well refer to the example of the Zero. Instead of using the world view that “Japanese aircraft were inferior copies of their own previous generation” to predicate their assessments, the U.S. War Department could have identified *the development of a technologically-advanced fighter aircraft by a non-friendly world power* as a key vulnerability construct through which information could be filtered. Having identified such vulnerabilities, the U.S. War Department could then have made assessments as to the likelihood of its eventuality and associated short, medium and long-term consequences. From there, a traditional risk management approach addressing mitigation of likelihood and consequences could have been instigated.

If such a process had been in place before the outbreak of the Pacific War in December 1941, the system may then have been ‘primed’ to be on the lookout for information indicating that this situation was actually developing. As further data were gathered, more accurate assessments of various probabilities and consequences could have been developed. This would have provided a framework that would have allowed the U.S. military intelligence system to more effectively integrate actual data into its worldview.

6.0 CONCLUSION

This paper examined how critical intelligence flows can be misused and overlooked by organisations and institutions. In doing this, it discussed formal (organizationally-embedded) and informal (non-organizationally-embedded) means of entry for intelligence flows, and the potential problems such variations can create. The work then detailed a historical example of this scenario from the Pacific Theatre of the Second World War and progressed to discuss how reduced analytical capacities to deal with unexpected sources (and forms) of intelligence might generate extreme surprise at an organizational level. A critical question examined here was how to expand organizational sensitivity in the face of broadening threat contexts – by accessing more diverse and non-traditional sources. Aligned to this was the need for

organizations to enhance flexibility in the way gathering and analysis of data was carried out in support of such sensitivity.

In approaching these questions the work examined a number of established self-defeating vulnerabilities within organizations and discussed ways of overcoming them. Critical to possible solutions to the inflexibilities noted in the paper are the use of multi-disciplined teams of analysts who not only assess threats but seek also to anticipate threat sources and emergence of harm by matching the variety and complexity of the threat environment with flexible analytic processes. In this way anticipation can be achieved by enhancing organisational capacity for contrasting threats against known organisational vulnerabilities. The study concluded by defining a conceptual framework based on anticipating the importance and meaning of incoming intelligence on threats in both the near and far term.

REFERENCES:

- Allinson, R.E. (1993) *Global Disasters: Inquiries into Management Ethics*, Prentice-Hall, New York.
- Ashby, W.R. (1968) *An Introduction to Cybernetics*, University Paperback, London.
- Beer, S. (1966) *Decision and Control*, Wiley, London.
- Byrd, M. (1987) *Chennault: Giving Wings to the Tiger*, University of Alabama Press, Tuscaloosa.
- Chennault, C.L. (1949) *Way of a Fighter: The Memoirs of Claire Lee Chennault*, G.P. Putnam's Sons, New York.
- Cross, R. (1987) *The Bombers: The Illustrated Story of Offensive Strategy and Tactics in the Twentieth Century*, Bantam Press, New York.
- Cull, B. and Sortehaug, P. (2004) *Hurricanes over Singapore*, Grub Street, London.
- Egan, T. (1989) 'Elements of tanker disaster: drinking, fatigue, complacency', *The New York Times*, May 22, B7.
- Francillon, R.J. (1987) *Japanese Aircraft of the Pacific War*, Naval Institute Press Annapolis, MA.
- Franks, N. (1986) *Aircraft versus Aircraft: The Illustrated Story of Fighter Combat since 1914*, Bantam Press, New York.
- Gunston, B. (1980) *An Illustrated Guide to German, Italian and Japanese Fighters of World War Two: Major Fighters and Attack Aircraft of the Axis Powers*, Salamander Books, London.
- Holmberg, S.C. (2001) 'An anticipatory searchlight approach', *International Journal of Computing Anticipatory Systems*, vol. 9, pp.70–83.
- Horikoshi, J. (1981) *Eagles of Mitsubishi: The Story of the Zero Fighter*, trans. Shindo, S. and Wantiez, H.N., University of Washington Press, Washington.
- Lagadec, P. (2004) 'Crisis: a watershed from local, specific turbulences, to global, inconceivable crises in unstable and torn environments, future crises', in *International Workshop, Future Agendas: An Assessment of International Crisis Research*.
- 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, École Polytechnique, Paris.
- Marais, K., Dulac, N. and Leveson, N. (2004) 'Beyond normal accidents and high reliability organizations: the need for an alternative approach to safety in complex systems',

- presented at the Engineering Systems Division Symposium, MIT, Cambridge, MA, March 29–31.
- Mason, R.O. (2004) ‘Lessons in organizational ethics from the Columbia disaster: can a culture be lethal?’, *Organizational Dynamics*, Vol. 33, No. 2, pp.128–142.
- Meyer, Herbert E. (2002) *Doing Intel: Lessons still unlearned*, (October 17, 9:00 a.m.) <http://nationalreview.com/comment/comment-meyer101702.asp>
- Mitroff, I.I., Alpaslan, M.C. and Murat, C. (2003) ‘Preparing for evil’, *Harvard Business Review*, Vol. 81, No. 4, pp.109–115.
- Mondey, D. (1996) *The Concise Guide to Axis Aircraft of World War II*, Chancellor Press, London.
- 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.
- Pearson, C.M. and Mitroff, I.I. (1993) ‘From crisis prone to crisis prepared: a framework for crisis management’, *Academy of Management Executive*, Vol. 7, No. 1, pp.48–59.
- Perrow, C. (1984) *Normal Accidents: Living with High Risk Technologies*, Basic Books, New York.
- Revans, R. (1982) *The Origins and Growth of Action Learning*, Chartwell-Bratt, Bromly.
- Sarewitz, D. and Pielke Jr., R. (2001) ‘Extreme events: a research and policy framework for disasters in context’, *International Geology Review*, Vol. 43, No. 5, pp.406–418.
- Schultz, D. (1987) *The Maverick War: Chennault and the Flying Tigers*, St. Martin’s Press, New York.
- Smart, C. and Vertinsky, I. (1977) ‘Designs for crisis decision units’, *Administrative Science Quarterly*, Vol. 22, No. 4, pp.640–657.
- Turner, B.A. and Pidgeon, N. (1997) *Man-made Disasters*, 2nd edn., Butterworth Heineman, Oxford.
- Voros, J. (2003) ‘A generic foresight process framework’, *Foresight*, Vol. 5, No.3, pp.10-21
- Weick, K. E. (1988) ‘Enacted sensemaking in crisis situations’, *Journal of Management Studies*, Vol. 25, No. 4, pp.304–313.
- Weir, D. (2004) ‘Sequences of failure in complex socio-technical systems: some implications of decision and control’, *Kybernetes*, Vol. 33, No. 3/4, pp.522–537.
- Wisnblit, J.Z. (1989) ‘Crisis management planning among U.S. corporations: empirical evidence and a proposed framework’, *S.A.M. Advanced Management Journal*, Vol. 54, No. 2, pp.31–41.

¹ Aspects of this contention are supported by the detail and analysis in the 9/11 Commission Report and assumptions of the presence of weapons of mass destruction (WMD) in Iraq as reasoning for military action there.

² ‘Sensemaking-’ follows the usage of Karl Weick and refers to a “Gestalt” of awareness enhancing understanding and decision-making under slow-burn and hot crisis conditions; see in particular Weick (1988).

³ And later the superlative ‘D’ model of the North American P-51 Mustang (operated by the USAAF), which was equipped with the Rolls Royce Merlin. Earlier Allison-engined Mustangs fought on roughly equal terms with the Zero. The Supermarine Spitfire Mk. V also fared poorly against the Zero, and it was not until the arrival of the more powerful Mk. VIII that the Spitfire (piloted by British and Australian airmen) could effectively match its opponent. The Vought Corsair was also operated by the USMC.

⁴ Chennault had retired with the rank of Captain in the USAAC Reserves; he had never held a rank higher than Major.

⁵ Extraordinary, too, is that an article in the September 1941 issue of the U.S. magazine *Aviation* stated that “America’s aviation experts can say without hesitation that the chief military airplanes of Japan are either outdated already, or are becoming outdated” (Schultz, 1987, 76). Of note, too, is that Chennault had personally informed General George C. Marshall, the Army’s chief of staff, of the threat posed by the Zero in late 1940. The latter even publicly spoke about this “new fast pursuit plane” in a press conference held the next day (Byrd, 1987, 111).

⁶ Referencing Beer (1966) and Revans (1982).