Working Paper: Signal and Noise in Early Warning

Chun Wei Choo
Faculty of Information Studies
University of Toronto

Abstract. This paper discusses the performance of early warning systems that are directed at hazards such as environmental, public health, and security threats. We introduce concepts from signal detection theory and organizational learning to analyze information acquisition and use in early warning programs. By attending to problems of signal detection, risk perception, and decision making bias, organizations can improve their capacity to sense and respond to emerging threats.

Introduction

In this paper, we focus on early warning systems that are directed at hazards such as environmental, public health, and security threats. We view early warning detection as a special case of environmental scanning (Choo 2002, 2006) in which knowledge about the threat is incomplete so that uncertainty is high; information about the threat is imperfect so that signals are ambiguous and hard to distinguish from noise; and timely action based on early detection is advantageous in managing the threat. Our discussion draws on concepts from signal detection theory and organizational learning.

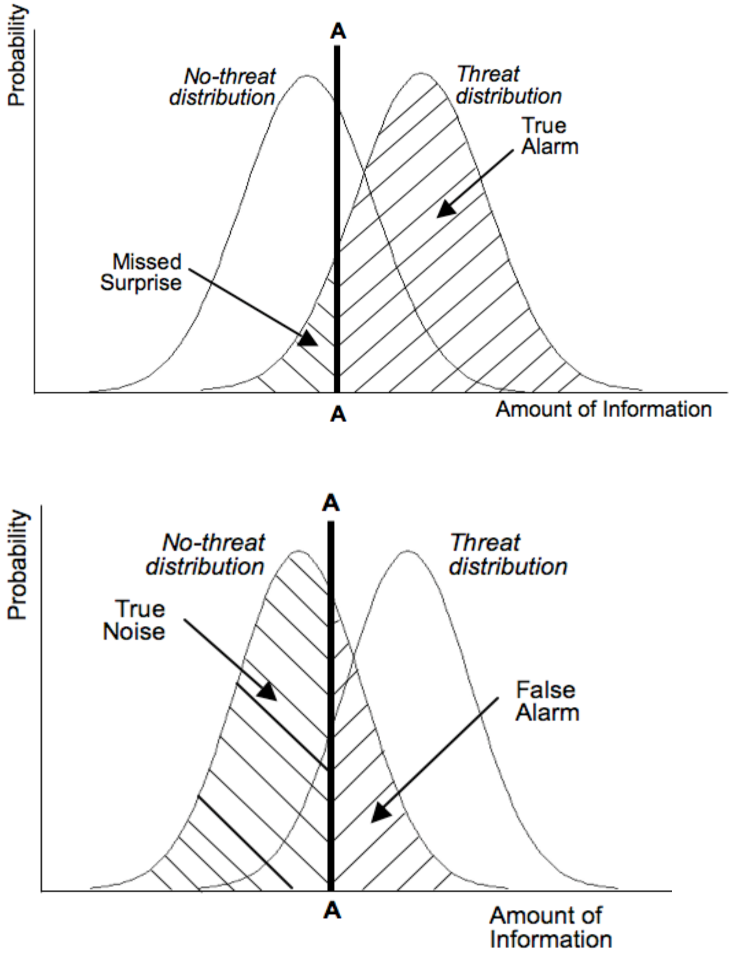
Signal Detection Theory

Signal Detection Theory (Green and Swets, 1966) is concerned with the problem of detecting a signal against a background of noise: how to analyze information in order to categorize ambiguous messages which can be generated by a known phenomenon (signal) or by chance (noise) (Abdi 2007). In an early warning situation, decision makers choose between whether a threat is present or not. The theory focuses on two aspects of this process: the strength of the signal relative to the noise; and the response strategy of the observer (Macmillan & Creelman 2005). When information about a threat is ambiguous and noisy, we may characterize the probability of receiving threat information as a normal distribution curve. In Figure 1, the x- and y-axis represent, respectively, the amount of information received (e.g. number of messages indicating possible threat), and the probability of receiving that amount of information. The curve on the left is the probability distribution of getting information when there is no signal (no threat). The right curve is the probability distribution of getting information when the threat is present. Assuming that there is more signal in the threat situation than the no-threat situation, the threat distribution is to the right of the no-threat distribution.

The strategy of the organization is expressed in its selection of an alarm-action threshold – the position on the x-axis (information axis) at which it takes action to deal with the imminent threat. In Figure 1, this threshold is the line AA: when the amount of information exceeds AA, the organization responds in anticipation of the threat. Because the threat and no-threat distributions overlap, the level of information indicated by AA can belong to either distribution. In the threat distribution (upper part of Figure 1), the shaded area under the curve to the right of AA represents the probability of true alarm while the area to its left is the probability of missed surprises. In the no-threat distribution (lower part of Figure 1), the shaded area to the right of AA represents the probability of false alarms while the area to its left is the true noise probability. A "risky" organization that shifts AA to the right (so that action is triggered at higher volumes of information) increases the risk of missed surprises but reduces the probability of false alarms.

Conversely, a "cautious" organization that moves AA to the left (so that action is triggered at lower volumes of information) reduces missed surprises but increases false alarms. The location of the AA threshold thus reflects how the organization has decided to balance the risks of missed surprises and false alarms.

Figure 1. Signal and Noise Distributions



Since knowledge and information about the threat is incomplete and imperfect, there is always overlap between the threat and no-threat distributions. Decreasing this overlap improves detection performance, reducing both false alarms and missed surprises. There are two general ways to do this: (1) increase the signal strength, thus increasing the separation between the threat and no-threat distributions; (2) reduce the noise or dispersion of both distributions, so that there is less overlap between two distributions that now have narrower shapes.

To increase signal strength we may expand the range and scope of information acquisition (Wagner et al 2001):

- scan more widely or scan existing areas more exhaustively;
- add sources that can provide early indicators of developing threats;
- monitor content in blogs and information sharing networks, e.g. Southeast Asia Earthquake and Tsunami blog, ProMED-mail (www.promedmail.org, International Society for Infectious Diseases);
- pay attention to the commentaries of mavericks and participants on the periphery.

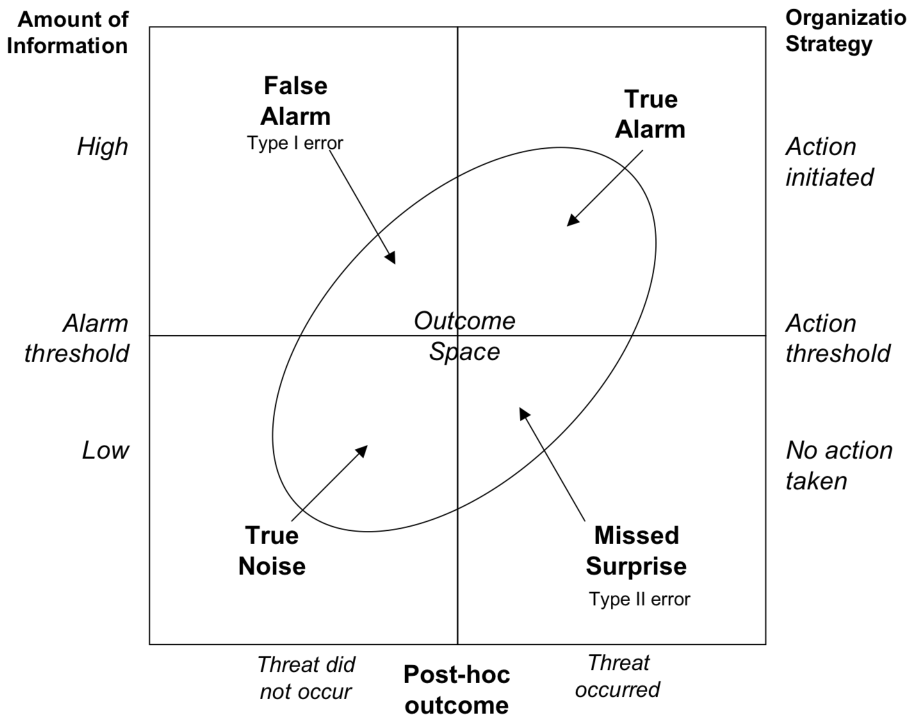
To reduce noise or amplify weak signals we might:

- focus additional information collection on areas that show significant activity;
- bring together groups of diverse, knowledgeable individuals to interpret information;
- use analytical tools to filter data and reveal patterns or trends, e.g. knowledge discovery, data visualization;
- aggregate information using prediction markets and wikis, e.g. Flu Prediction Market (www.biz.uiowa.edu/IEM/fluprediction, University of Iowa), Intellipedia (US intelligence community).

Organizational Learning

We summarize our discussion so far in Figure 2 (adapted from Shapira, 1995; Lampel and Shapira, 2001). Since organizational strategy is triggered through the selection of the alarm-action threshold, an organization should be able to learn from experience and rely on objective evidence in setting a threshold that minimizes error. However, learning to recognize and respond to risky threats presents special challenges. We consider three impediments: the false alarm bias, the dread risk bias, and the difficulty of learning from rare events.

Figure 2. Early Warning Framework



(1) False alarm bias

In Figure 2, the outcome space bounds the four action-outcome combinations. Its elliptical shape reflects incomplete knowledge about the threat. If knowledge is perfect, the ellipse becomes a straight line of perfect correlation between information and outcome. If knowledge is lacking, it would look more like a circle (Shapira 1995). For a given state of knowledge we can either minimize false alarms (Type I error) or minimize missed surprises (Type II error) *but not both*: decreasing the likelihood of one error necessarily increases the likelihood of the other. Moreover, the costs of the two types of errors are rarely symmetrical in early warning situations (Puranam et al 2006). An alarm that initiates action which is disruptive and unpopular (e.g., closure of offices, schools, transportation) may be perceived as having high economic and social costs. When the costs of false alarms are expected to be prohibitive, analysts and decision makers may weigh heavily the probability of false alarms when setting the threshold. Decision makers also over-emphasize recent false alarms when considering whether to act. A string of recent alerts where the threat did not materialize may increase the tendency to avoid another costly false alarm.

(2) Dread risk bias

Slovic (1987) found that risk perception is characterized by three factors: "dread risk" defined as risk that is high in perceived lack of control, dread, catastrophic potential, fatal consequences, and inequitable distribution of risks; "unknown risk" defined as risk perceived to be unobservable, unknown, new, and delayed in their manifestation of harm; and the number of people exposed to the risk. For laypeople, the most important factor is "dread risk." The higher the dread factor, the higher the perceived risk, the more people want to see the threat reduced, and the more they want to see strict regulation employed to attain this. A related idea is the use of the "precautionary principle" which states that regulators should take steps to protect against potential harms, even if we do not know the likelihood and the cause-effect basis of these dangers (Sunstein 2005). People single out certain risks as "salient," based on their ability to recall instances of those risks, particularly well-publicized and emotionally charged instances that can exaggerate a risk. The combined effect of dread risk and the precautionary principle is that decision makers lower the action threshold, increasing the probability of false alarms.

(3) Small sample learning

Given that mishaps occur infrequently, how can organizations maximize learning from limited experience? March, Sproull and Tamuz (1991) propose two strategies. First, organizations can enhance the *richness* of sparse experience by focusing intensively on critical incidents – close examination of these incidents can reveal hidden features and suggest better ways to manage them. Richness is also gained by including the interpretations of different participants, thereby learning different lessons from the same experience. Organizations can clarify values and preferences about what distinguishes successes from failures by reflecting on the consequences of their actions. Second, organizations can *simulate* experience by learning from events that almost happened or might have happened. Thus, information on near-misses is collected to augment the history of real accidents and to identify weaknesses. Alternative scenarios of what could have happened constructed from specific events can also help the organization plan for different threat trajectories. All the activities enumerated above require resources, and a genuine organizational commitment to learning.

Coda

This paper introduced concepts from signal detection theory and organizational learning to analyze information acquisition and use in early warning activities. By attending to problems of signal detection, risk perception, and decision making bias, organizations can improve their capacity to sense and respond to developing threats.

References

Abdi, H. (2007). Signal Detection Theory. In N. Salkind (Ed.), Encyclopedia of Measurement and Statistics (pp. 886-889). Thousand Oaks, CA: Sage.

Choo, C.W. (2002). Information Management for the Intelligent Organization: The Art of Scanning the Environment (3rd ed.). Medford, NJ: Information Today, Inc.

Choo, C.W. (2006). The Knowing Organization: How Organizations Use Information to Construct Meaning, Create Knowledge, and Make Decisions (2nd ed.). New York: Oxford University Press.

Green, D.M., & Swets, J.A. (1966). Signal Detection Theory and Psychophysics. New York: John Wiley.

Lampel, J., & Shapira, Z. (2001). Judgmental Errors, Interactive Norms, and the Difficulty of Detecting Strategic Surprises. Organization Science, 12(5), 599-611.

Macmillan, N.A., & Creelman, C.D. (2005). Detection Theory: A User's Guide (2nd ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

March, J., Sproull, L., & Tamuz, M. (1991). Learning From Samples of One or Fewer. Organization Science, 2(1), 1-13.

Puranam, P., Powell, B.C., & Singh, H. (2006). Due Diligence Failure as a Signal Detection Problem. Strategic Organization, 4(4), 319.

Shapira, Z. (1995). Risk Taking: A Managerial Perspective. New York: Russell Sage Foundation.

Slovic, P. (1987). Perception of Risk. Science, 236, 280-285.

Sunstein, C.R. (2005). Laws of Fear: Beyond the Precautionary Principle. Cambridge, UK: Cambridge University Press.

Wagner, M.M., Tsui, F.C., Espino, J.U., Dato, V.M., Sittig, D.F., Caruana, R.A., et al. (2001). The Emerging Science of Very Early Detection of Disease Outbreaks. Journal of Public Health Management Practice, 7(6), 51-59.